GROUPES

Classification Thèmes de MégaMaths

Docs de Dany-Jack MERCIER

Groupes opérant sur un ensemble.
groupes de SYLOW

(Dany-Jack MERCIER, 1979)
[ugpe-groupesdesylow.pdf]

Définition - Équation des classes.

On dit qu'un groupe G opère sur un ensemble E, à gauche, si ∃ loi externe

$$G \times E \longrightarrow E$$
$$(g, x) \longmapsto g.x$$

qui vérifie :
1) $g.(g'.x) = (gg').x \quad \forall g, g' \in G \ \forall x \in E$
2) $e.x = x \quad \forall x \in E$

Th | L'ensemble E est un G-ensemble si et seulement si G est homomorphe au groupe S(E)

NB : S(E) est le groupe symétrique de E, c.à.d le groupe de toutes les permutations de E dans E, muni de $\circ$.
L'homomorphisme $T : G \to S(E)$ annoncé n'est autre que $T_g(x) = g.x$.

Définitions :

a) G opère fidèlement sur E si $T : G \to S(E)$ est injectif,
c.à.d si $gx = x \ \forall x \in E \Rightarrow g = e$

b) $G_x = \{ y \in E / \exists g \in G \quad y = g.x \}$ = orbite de x pour le groupe G.

c) $H_x = \{ g \in G / gx = x \}$ est un sous-groupe de G. C'est le sous-groupe d'isotropie, ou "stabilisateur" de x dans G.

Th | Soit Ω une orbite pour G. Si x et y sont éléments de Ω, alors les groupes d'isotropie H_x et H_y sont conjugués dans G.

On remarque que la relation dans E : $x \sim y \Leftrightarrow \exists g \in G \quad y = gx$ est une relation d'équivalence, et que les classes de $\sim$ ne sont autres que les orbites dans E :
plus précisemment : $\dot{x}_{(\sim)} = G_x$
Les orbites de E forment donc une partition de E.
Montrons le théorème :

Donc : $x, y \in \Omega = G_z \Leftrightarrow \exists \sigma \in G \quad x = \sigma.y$

$$h \in H_x \Leftrightarrow h.x = x \Leftrightarrow (h\sigma).y = \sigma.y \Leftrightarrow (\sigma^{-1}h\sigma).y = y$$
$$\Leftrightarrow \sigma^{-1}h\sigma \in H_y \Leftrightarrow h \in \sigma H_y \sigma^{-1}$$

d'où $H_x = \sigma H_y \sigma^{-1}$, ce qui signifie que le sous-groupe H_x est le conjugué de H_y.
CQFD

$g \mapsto g \cdot x$

f_x se factorise canoniquement puisque :

$$f_x(g_1) = f_x(g_2) \Leftrightarrow g_1 \cdot x = g_2 x \Leftrightarrow g_2^{-1} g_1 \cdot x = x \Leftrightarrow g_2^{-1} g_1 \in H_x$$

Ainsi, le diagramme suivant est commutatif :

$$\begin{array}{ccc} G & \xrightarrow{f_x} & f_x(G) = G_x \\ \pi \downarrow & \nearrow & \\ G/H_x & & \end{array}$$

θ ~~homo~~ bijectif.

G/H_x : classes à gauche suivant le sous-groupe d'isotropie H_x.

Ainsi, si G est fini : $\# G_x = \# G/H_x = \dfrac{\# G}{\# H_x}$

$$\boxed{\# G_x = \frac{\# G}{\# H_x}}$$

<u>Equation des classes</u> :

Si l'ensemble E est fini, chaque orbite est un ensemble fini. Si $E' \subset E$, E' ne contient qu'un élément et un seul de chaque orbite, alors, eu égard à la partition réalisée par la relation $\sim$ dans E :

$$\boxed{\# E = \sum_{x \in E'} \# G_x = \sum_{x \in E'} \frac{\# G}{\# H_x}}$$ (équation des classes)

<u>Exemple</u> : G groupe fini. $\varphi : G \to \mathrm{Int}(G) \subset S(G)$, $g \mapsto \varphi_g \;/\; \varphi_g(x) = g x g^{-1}$

φ est un épimorphisme de groupes.

C'est donc un G-ensemble pour la loi dite de conjugaison : $G \times G \to G$, $(g, x) \mapsto g x g^{-1}$

H_x = stabilisateur de $x = \{ g \in G \;/\; gx = xg \}$

Si $z \in Z(G)$ $H_z = G$ et réciproquement. Donc $\# G_z = 1$

L'équation des classes implique : $\# G = \sum_{x \in Z(G)} \# G_x + \sum_{x \in A} \# G_x$

(A = ensemble des éléments de G tel que 2 éléments quelconques de A ne sont pas conjugués). Ainsi :

$$\boxed{\# G = \# Z(G) + \sum_{x \in A} \# G_x}$$

<u>exercice</u> : $p \in \mathcal{P}$, G groupe d'ordre p^k. Alors $Z(G)$ n'est pas trivial.

[Sol : Pour $x \notin Z(G)$, Card G_x divise proprement p^k donc est une puissance de p.
On a $\# Z(G) = \# G - \sum_{x \notin Z(G)} \# G_x \Rightarrow \# Z(G) \equiv 0 \; [p] \Rightarrow Z(G)$ non trivial]
(Théorème de Burnside)

groupes primaires, groupes de Sylow   1°/ Définitions et premières propriétés.

Th 1 | Tout groupe fini commutatif contient un élément d'ordre $p \in \mathcal{P}$ si $p | \# G$

Th 2 | Soit G un groupe fini d'ordre n, et $p \in \mathcal{P}$ / $p^k | n$.
Alors G contient un sous-groupe d'ordre p^k

preuve: le théorème est trivial si $n = p^k$.
On raisonne par récurrence sur n en supposant le théorème vrai pour tous les groupes d'ordre $n' < n$.
G est un G-ensemble pour la loi de conjugaison $(g, x) \longmapsto gxg^{-1}$.
De 2 choses l'une :

a) $\exists x \notin Z(G) / \# G_x \not\equiv 0 \; [p]$. Alors $n = \# H_x \cdot \# G_x$
p, premier, est premier avec tout nombre qu'il ne divise pas. Donc $\Delta(p^k, \# G_x) = 1$ et le théorème de Gauss donne : $p^k | \# H_x$. H_x, stabilisateur de x, est un sous-groupe de G d'ordre $\# H_x = \frac{n}{\# G_x} < n$ puisque $\# G_x > 1$.
D'après l'hyp. de récurrence :

H_x possède un sous-groupe d'ordre p^k

b) $\forall x \notin Z(G) / \# G_x \equiv 0 \; [p]$.
L'équation des classes donne :

$$\# Z(G) = n - \sum_{x \in A} \# G_x \equiv 0 \quad [p]$$

Le centre Z(G) n'est pas trivial. Comme $p | \# Z(G)$, il existe selon le th. 1 un élément $a \in Z(G)$ d'ordre p. Le groupe $\langle a \rangle = H$ est d'ordre p. Il est distingué dans G, puisque $H \subset Z(G)$.

$p^k | n \Rightarrow p^{k-1} | \# (G/H)$

D'après l'hypothèse de récurrence, $\exists K' \subset G/H$ K' sous-groupe d'ordre p^{k-1}
Soit $\pi : G \to G/H$ et $K = \pi^{-1}(K')$. $K \supset H$ et $\pi|_K : K \longrightarrow K'$
donc $K/H \simeq K' \Rightarrow \# K = p^k$

$K \downarrow K/H \nearrow$ ≃ groupes

CQFD

Def | Soit p un nombre premier.

- Un p-groupe (ou groupe p-primaire) est un groupe fini d'ordre p^α
- Si $H \subset G$, H est un p-groupe, on dira que c'est un p-sous-groupe de G.
- Si $H \subset G$ est un p-sous-groupe de G de cardinal p^n où p^n est la plus grande puissance de p qui divise $\# G$, alors H sera dit " un p sous-groupe de Sylow.

(NB : $H \subset G$ est un p sous-groupe de Sylow ssi c'est un p-sous-groupe maximal.)

Co | Soit G un groupe fini et $p \in \mathcal{P}$ $p | \# G$. Alors il existe un p-sous-groupe de Sylow de G.

① Tout conjugué d'un p sous-groupe de Sylow est encore un p sous-groupe de Sylow.

[$H \subset G$ $\# H = p^n$ où $\# G = n = p^n m$ $\Delta(p,m) = 1$. $H' = gHg^{-1} = \varphi_g(H)$ où $\varphi_g(x) = gxg^{-1}$ est un automorphisme intérieur. φ_g est bijectif, donc conserve le cardinal].

② Soit G un groupe abélien fini de cardinal n.

$$\exists m \in \mathbb{N}^* \ / \ \forall g \in G \quad mg = 0 \quad \Rightarrow \exists k \in \mathbb{N} \quad n \mid m^k$$

[Par récurrence sur m. Soit $g \in G$, $g \neq 0$ et $H = \langle g \rangle$. $\# G/H < n$
G/H est un groupe, et $m\dot{g} = \dot{0}$ $\forall \dot{g} \in G/H$. D'après l'hypothèse de récurrence, $\# G/H \mid m^k$ or $\# G/H = \frac{\# G}{\# H} = \frac{n}{\# H}$ et $\# H \mid m$

d'où $\frac{n}{\# H} \mid m^k \Leftrightarrow m^k = \lambda \frac{n}{\# H}$ et $m = \mu \# H$ d'où $m^{k+1} = \mu \lambda n \Leftrightarrow n \mid m^{k+1}$]

Th 3 | Si P est un p sous-groupe de Sylow d'un groupe fini, alors tout p-sous-groupe de N(P) est contenu dans P.

(Rappel : $N(H) = \{ g \in G \ / \ gHg^{-1} = H \}$)

preuve : Soit R un p sous-groupe contenu dans N(P). Comme $P \triangleleft N(P)$ et $R \subset N(P)$
$R/_{P \cap R} \simeq PR/_P$. Or $\#(R/_{P\cap R}) = p^\alpha \Rightarrow \# PR/_P = p^\alpha$ et a fortiori $\#(PR) = p^\beta$
P.R est donc un p-groupe de G, et il contient P. Mais P est un p sous-groupe de Sylow, donc maximal parmi les p-sous-groupes, d'où $PR = P \Rightarrow R \subset P$

Th 4 | Soit H un sous-groupe du groupe fini G
Alors :

H = p-sous-groupe de Sylow $\Leftrightarrow$ H = maximal dans l'ensemble des p-groupes de G ordonné par l'inclusion.

($\Rightarrow$) $\# H = p^k$ où $n = p^k m$ $\Delta(m,p) = 1$.
Soit K un p-sousgroupe de G contenant H. $\# K = p^\alpha$

$$\left.\begin{array}{l} H \subset K \Rightarrow k \leq \alpha \\ K \text{ sous-groupe de } G \Rightarrow \alpha \leq k \end{array}\right\} \Rightarrow \# K = p^k = \# H \Rightarrow H = K$$

Donc H est maximal.

($\Leftarrow$) notons $\# H = p^\alpha$. d'autre part il existe $K \subset G$ / $\# K = p^k$ où $n = p^k . m'$ ($\Delta(m', p) = 1$). considérons $\Lambda = \{ x \in G \ / \ x^{p^k} = e \}$. alors on rem. que Λ est un p-sous-groupe de G, et que $H \subset \Lambda$. H étant maximal, on a donc $H = \Lambda$. or $K \subset \Lambda = H$ d'où (à cause des cardinaux), $K = H$, H est donc un p-sous-groupe de Sylow.

2°/ Théorème de Cauchy

On généralise le Th 1 précédent :

Th (de Cauchy) Soit G un groupe fini d'ordre n et p un diviseur premier de n. G possède un élément d'ordre p.

preuve : récurrence sur $\# G = n$. Si $n = 2$, $G = \mathbb{Z}/2\mathbb{Z}$ et l'assertion est vraie.
Supposons la démontrée pour tout $m < n$. Soit $p \mid n$, $p \in \mathcal{P}$.
Si $G = Z(G)$, le résultat est vrai (cf. Th 1)
Supposons $G \neq Z(G)$. De 2 choses l'une :

a) $\exists x \in G \setminus Z(G)$ tel que $p \mid \# H_x$

(Ici, H_x = stabilisateur de x pour la conjugaison $= \{ g \in G / \ g^{-1} x g = x \}$ on le nomme aussi le centralisateur de G.)
Mais $x \notin Z(G) \Rightarrow H_x \subsetneq G \Rightarrow \# H_x < \# G$ et d'après l'hypothèse de récurrence, il existe un élément d'ordre p dans H_x, donc dans G.

b) $\forall x \in G \setminus Z(G)$, $p \nmid \# H_x$

Mais $p \in \mathcal{P}$ divise $n = \# G = \# G/_{H_x} \cdot \# H_x$ et $p \nmid \# H_x$, donc $p \mid \# G/_{H_x}$ pour tout $x \notin Z(G)$
D'après l'équation des classes :

$$\# G - \sum_{x \in A} \# G/_{H_x} = \# Z(G)$$

donc $p \mid \# Z(G)$ et $Z(G)$ est commutatif ! le Th 1 nous donne l'existence d'un élément d'ordre p dans $Z(G)$, donc dans G.
CQFD

Exemple : Dans $\mathcal{S}_4$, il y a un élément d'ordre 2 et un d'ordre 3.
En effet : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Ce théorème permet de donner une équivalence précieuse entre définitions :

Pro Soit G un groupe fini. Alors :

$$\# G = p^k \Leftrightarrow \{ \forall x \in G \ \exists \alpha \in \mathbb{N} \quad p^\alpha x = 0 \}$$

(NB : d'où une autre définition d'un p-groupe, si G est un groupe fini. Dans le cas où G est infini, G est dit p-groupe si $\forall x \in G \ \exists \alpha / \ \omega(x) = p^\alpha$, et la définition de "droite" s'avère plus généralisable ...)

- Si $\# G = p^k$ $\forall x \in G$ $\langle x \rangle \subset G \Rightarrow \omega(x) = p^\alpha$ (Th. Lagrange)
- Inversement, si $\forall x \in G$ $\exists \alpha$ $p^\alpha x = 0$, supposons que $q \in \mathcal{P}$ $q \mid \# G$

D'après le théorème de Cauchy ci-dessus, G possède un élément d'ordre q. Donc $\exists \alpha / \ q = p^\alpha$ et $q \in \mathcal{P} \Rightarrow \alpha = 1$. Ainsi $q = p \Rightarrow \# G = p^k$.

3°/ Dénombrement des p-groupes de Sylow

Th 5 Deux p-sous-groupes de Sylow d'un groupe fini G sont conjugués dans G.
Le nombre de p-sous-groupes de Sylow de G est de la forme $1 + kp$.

(NB : on sait déjà que si H est un p-sousgroupe de Sylow, alors tous les conjugués de H sont aussi des p-sous-groupes de Sylow)

. parties :

1-partie : On montre que $\# \mathcal{O} = r \equiv 1 [p]$

G opère sur $\mathcal{H}$ ensemble des sous-groupes de G, par conjugaison : $G \times \mathcal{H} \longrightarrow \mathcal{H}$, $g, H \longmapsto gHg^{-1}$

P = sgroupe de Sylow

$N(P) = G_P = \{g \in G / gPg^{-1} = P\}$ = groupe d'isotropie, ou stabilisateur, de P.
(NB : ici, il est égal au normalisateur de P)

On désigne par $\mathcal{O}$ l'orbite de P. On a : $\# \mathcal{O} = r = \#G / \#N(P)$

P opère sur $\mathcal{O}$ par conjugaison : $P \times \mathcal{O} \longrightarrow \mathcal{O}$, $h, H \longmapsto hHh^{-1}$

Soit $\mathcal{U}$ l'orbite de P sous cette action.

$$\mathcal{U} = \{O \in \mathcal{O} / \exists h \ hPh^{-1} = O\} = \{P\}$$

Ainsi $\# \mathcal{U} = 1$.

Soit $\mathcal{U}_i$ = orbite de $P_i \in \mathcal{O}$, pour $P_i \neq P$.

Si $\# \mathcal{U}_i = 1 \Rightarrow hP_ih^{-1} = P_i \ \forall h \in P \Rightarrow P \subset N(P_i)$ et d'après le théorème 3 : $P \subset P_i$ (car P = p-sous-groupe).

Comme P est maximal dans l'ensemble des p-groupes $P \subset P_i \Rightarrow P = P_i$, ce qui est absurde.

Donc $P_i \neq P \Rightarrow \# \mathcal{U}_i \neq 1$. L'équation des classes donne :

$$\# \mathcal{O} = r = 1 + \sum_{P_i \neq P} \# \mathcal{U}_i$$

Notons H_i le stabilisateur de P_i sous l'action de P opérant sur $\mathcal{O}$ par conjugaison :

$$\# \mathcal{U}_i = \#P_i / \#H_i \Rightarrow \# P_i = (\# \mathcal{U}_i)(\# H_i) \Rightarrow \# \mathcal{U}_i \equiv 0 \ [p]$$

($\# \mathcal{U}_i \neq 1$ et P_i = p-s.groupe de Sylow)

d'où $r \equiv 1 [p]$. ($r = \# \mathcal{O}$) (1)

2-partie : Tous les p-sgroupes de Sylow sont dans $\mathcal{O}$.

Soit Q un p-sous-groupe de Sylow non conjugué à P. Cela revient à dire que $Q \notin \mathcal{O}$

Q opère par conjugaison sur $\mathcal{O}$ $\quad Q \times \mathcal{O} \longrightarrow \mathcal{O}$, $(q, O) \longmapsto qOq^{-1}$

Si $\mathcal{V}_i$ = orbite de $P_i \in \mathcal{O}$, alors $\forall P_i \in \mathcal{O}$: $\# \mathcal{V}_i \neq 1$

[$\# \mathcal{V}_i = 1 \Rightarrow \forall q \in Q \ qP_iq^{-1} = P_i \Rightarrow Q \subset N(P_i) \Rightarrow Q \subset P_i$ (th3)
donc $Q = P_i$ (cf. Q maximal)
Donc $\# \mathcal{V}_i \neq 1$]

L'équation des classes est ici : $\# \mathcal{O} = \sum \# \mathcal{V}_i$ où $\# \mathcal{V}_i = \dfrac{\#Q}{\#(\text{stabilisateur de } P_i)}$

$\# \mathcal{V}_i \neq 1 \Leftrightarrow \# \mathcal{V}_i > 1 \Rightarrow \# Q > \#(\text{stabilisateur de } P_i)$.

Comme $\#Q = p^n$ et que (stabilisateur de P_i) $\subset Q$ est de cardinal p^α, et comme $p^n > p^\alpha$, on en déduit que $\# \mathcal{V}_i \equiv 0 \ [p]$.

Donc $\# \mathcal{O} = \sum \# \mathcal{V}_i \equiv 0 \ [p]$ ce qui est absurde selon (1) !

Conclusion : Q = p sous-groupe de Sylow $\Rightarrow Q \in \mathcal{O}$ (orbite de P)
et $\# \mathcal{O} = r \equiv 1 [p]$.

Pro | Soit G un p-groupe.
1) Alors $Z(G) \neq \{e\}$
2) G est résoluble.

preuve : 1) On considère l'équation des classes pour l'opération de conjugaison :

$G \times G \to G$

$(g, x) \mapsto gxg^{-1}$ $\quad \# G = \# Z(G) + \sum_{x \in A} \frac{\# G}{\# H_x}$ (avec $\# H_x = \# G_x$)

Comme $\# G = p^n$, $G_x \subset G \Rightarrow \# G_x \mid p^n$

et $\# G_x \neq p^n$ (sinon $G_x = G$ et $Z(G) = G$!) Donc $\# Z(G) \equiv 0 \; [p]$. (1)

2) Gest résoluble.

Récurrence sur $\# G$.

- vrai pour $\# G = 2$ car $G = \mathbb{Z}/2\mathbb{Z}$ résoluble car commutatif.
- $Z(G) \subset G$ est un sgroupe de G et $\# G/Z(G) < \# G$ d'après (1)

Alors :

$$G/Z(G) = G'_0 \supset G'_1 \supset \ldots \supset G'_n = \{e\} \quad (2)$$

où $G'_{k+1} \lhd G'_k$ et G'_k / G'_{k+1} commutatif

Notons $\pi : G \to G/Z(G)$. On pose $G_i = \pi^{-1}(G'_i)$. On sait que π est une bijection croissante de l'ensemble des sous-groupes contenant $Z(G)$ sur l'ensemble des sous-groupes de $G/Z(G)$. Ainsi (2) $\Rightarrow$

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \pi^{-1}(e) = Z(G)$$

et $\begin{cases} \cdot \; G_{k+1} \lhd G_k \\ \cdot \; G_k / G_{k+1} \simeq G'_k / G'_{k+1} \end{cases}$

CQFD

[NB : • $\forall x \in G_k \; \forall g \in G_{k+1}, \; \dot{\overline{xgx^{-1}}} \in G'_{k+1} \Rightarrow \dot{\overline{xgx^{-1}}} = \dot{g}' \quad g' \in G_{k+1}$

c.à.d $xgx^{-1} g'^{-1} \in Z(G) \subset G_{k+1} \Rightarrow xgx^{-1} \in G_{k+1}$.

• Considérons $\pi : G_i / G_{i+1} \longrightarrow G'_i / G'_{i+1}$. C'est un isomorphisme.

$\dot{x} \longmapsto \overline{\pi(x)}$

* π est bien défini car $\dot{x} = \dot{y} \Leftrightarrow xy^{-1} \in G_{i+1} \Rightarrow \pi(x)\pi(y)^{-1} \in G'_{i+1} \Leftrightarrow \overline{\pi(x)} = \overline{\pi(y)}$
* π surjective.
* π injective : car $\begin{cases} \overline{\pi(x)} = \bar{0} \Leftrightarrow \pi(x) \in G'_{i+1} \Leftrightarrow x \in G_{i+1} \\ x \in G_i \end{cases} \Rightarrow \dot{x} = \dot{0}$.]

Décomposition d'un groupe commutatif fini

(Dany-Jack MERCIER, 1979)
[ugpe-decompositiondungroupecommutatiffini].pdf

I Définition d'un p-groupe

Def | Soit G un groupe. On dit que G est un p-groupe si son cardinal est une puissance de p ($p \in \mathcal{P}$).

Th | Soit G un groupe commutatif fini.
Alors $G = p\text{-groupe} \Leftrightarrow \{\forall x \in G\ \exists \alpha \in \mathbb{N}\ /\ \omega(x) = p^\alpha\}$

preuve : • Supposons que $\forall x \in G\ \omega(x) = p^\alpha$. On fait une récurrence sur le cardinal de G. En notation additive :

→ Pour $G = \{0\}$, c'est évident

→ Soit G de cardinal n. Soit $x \in G$, $x \neq 0$. Notons $H = \langle x \rangle$. C'est un groupe cyclique d'ordre p^k. Mais $\# G = \# H \cdot \# G/_H$ et $G/_H$, groupe commutatif, vérifie $\forall \dot{x} \in G/_H\ \exists \alpha\ /\ p^\alpha \dot{x} = \dot{0}$. De plus $\# G/_H < \# G$. L'hypothèse de récurrence s'applique : $\# G/_H = p^\beta$. Comme $\# H = p^k$, on trouve que $\# G = p^{\beta+k}$ cqFd

• Inversement, si G est un p-groupe, $\# G = p^k$ et tout élément x de G engendre $\langle x \rangle$ d'ordre $p^\alpha \mid p^k$. Par suite $\omega(x) = p^\alpha$.

II Décomposition en p-groupes (ou "composantes p-primaires")

Th | Soit G un groupe commutatif fini d'ordre $n = p_1^{r_1} \cdots p_k^{r_k} = q_1 \cdots q_k$
Posons $G(p_i) = \{x \in G\ /\ q_i x = 0\}$
$G(p_i)$ est un p_i-groupe et :

$$G = G(p_1) \oplus \cdots \oplus G(p_k)$$

Il est clair que $G(p_i)$ est un groupe, et que $\forall x \in G(p_i)\ \ \omega(x) \mid p_i^{r_i} \Rightarrow \omega(x) = p_i^\alpha$
donc $G(p_i) = p_i$-groupe.

Montrons la somme directe :

* $\forall x \in G\ \ \exists x_i \in G(p_i)\ /\ x = x_1 + \cdots + x_k$?

Il est clair que $\Delta\left(\frac{n}{q_1}, \frac{n}{q_2}, \ldots, \frac{n}{q_k}\right) = 1 \Leftrightarrow \sum_{i=1}^{k} m_i \frac{n}{q_i} = 1$ (Bezout)

Donc $x = \underbrace{m_1 \frac{n}{q_1} x}_{\in G(p_1)} + \cdots + \underbrace{m_k \frac{n}{q_k} x}_{\in G(p_k)}$

Donc $G = G(p_1) + \cdots + G(p_k)$

* $\forall j \in [1, k]\quad G(p_1) + \cdots + G(p_{j-1}) \cap G(p_j) = \{0\}$?

Soit $x \in G(p_1) + \cdots + G(p_{j-1}) \cap G(p_j)$ où $j \in [1, k]$

Alors $q_j x = 0$ et $x = x_1 + \cdots + x_{j-1}$ où $x_i \in G(p_i) \Leftrightarrow q_i x_i = 0\ \ \forall i$

Soit $s = \prod_{i=1}^{j-1} q_i$. On a $sx = 0$

q_j et s sont premiers entre eux ! donc $\lambda q_j + \mu s = 1 \Rightarrow x = \lambda q_j x + \mu s x = 0$

CQFD

décomposition en p-groupes cycliques.

Énonçons tout d'abord :

Th 1 | Tout p-groupe commutatif G se décompose en groupes cycliques p-primaires,
$$G \simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z} \qquad \alpha_1 \leq \dots \leq \alpha_s$$
De plus, la suite $(\alpha_1, \dots, \alpha_s)$ est unique.

Soit G un p-groupe commutatif. Énonçons 2 lemmes :

lemme 1 : $\left.\begin{array}{l} b \in G \quad b \neq 0 \quad p^k b \neq 0 \\ \omega(p^k b) = p^m \end{array}\right\} \Rightarrow \omega(b) = p^{m+k}$

lemme 2 : Soit $a_1 \in G$ $G_1 = \langle a_1 \rangle$ / $\# G_1 = p^{r_1} = \operatorname{Sup}\{\omega(x) / x \in G\}$
Soit $\dot{b} \in G/G_1$ tel que $\omega(\dot{b}) = p^r$. On pose $\pi_1 : G \to G/G_1$
Alors $\exists b$ / $\pi_1(b) = \bar{b}$ et $\omega(b) = p^r$.

preuve lemme 1 : On a $\left\{\begin{array}{l} p^{m+k} b = 0 \\ p^{m+k-1} b = p^{m-1}(p^k b) \neq 0 \text{ car } \omega(p^k b) = p^m \quad (m \geq 1) \end{array}\right.$
donc $\omega(b) = p^{m+k}$

preuve lemme 2 : Soit $b \in G$ tel que $\pi_1(b) = \bar{b}$. π_1 est un morphisme de groupes, donc il abaisse les ordres des éléments : $\omega(b) \geq p^r$, $\forall b \in \pi_1^{-1}(\bar{b})$. $(*)$
On a $p^r b \in G_1 \iff p^r b = n a_1$ où $0 \leq n < p^{r_1}$
$p^r b = p^k \mu a_1$ où $p \nmid \mu$ $(k < r_1)$
$\omega(p^k \mu a_1) = \dfrac{p^{r_1}}{\Delta(p^k\mu, p^{r_1})} = p^{r_1 - k}$ et $p^r b \neq 0 \underset{\text{(lemme 1)}}{\Longrightarrow} \omega(b) = p^{r+r_1-k}$
Comme $r_1 = \operatorname{Sup}\{\omega(x) / x \in G\}$ et que $\omega(b) = p^{r+r_1-k}$, on aura forcément l'inégalité : $r + r_1 - k \leq r_1 \iff r \leq k$
Par suite : $p^r b = p^k \mu a_1 \Rightarrow (b - p^{k-r}\mu a_1) p^r = 0 \Rightarrow \omega(b - p^{k-r}\mu a_1) = p^r$ (cf. $(*)$)
On a qu'à prendre $b' = b - p^{k-r}\mu a_1 \in \pi^{-1}(\dot{b})$

preuve du théorème :

• Existence de la décomposition

$\# G = p^u$. On fait une récurrence sur u.
C'est vrai pour $u = 1$. Soit G de cardinal $\# G = p^u$. Alors $\# G/G_1 = p^{u - r_1}$
et l'on peut appliquer l'hypothèse de récurrence :
$$G/G_1 = \bar{G}_2 \oplus \dots \oplus \bar{G}_s \quad \text{où } \bar{G}_i = \dot{a}_i \mathbb{Z} \quad \omega(\dot{a}_i) = p^{r_i}$$
(groupes cycliques primaires)

D'après le lemme 2 :
$$\exists a_i \in G \quad / \quad \pi(a_i) = \dot{a}_i \quad \text{et} \quad \omega(a_i) = p^{r_i}$$
Posons $G_i = a_i \mathbb{Z} = \langle a_i \rangle$ et montrons que $G = G_1 \oplus \dots \oplus G_s$:
1) $G = G_1 + \dots + G_s$
En effet, $\forall x \in G$ $\dot{x} = m_2 \dot{a}_2 + \dots + m_s \dot{a}_s \iff x = \underbrace{m_1 a_1}_{\in G_1} + \dots + m_s a_s$.
2) Si $m_1 a_1 + \dots + m_s a_s = 0$ $\quad 0 \leq m_i < p^{r_i}$
alors $m_2 \dot{a}_2 + \dots + m_s \dot{a}_s = 0$ d'où $m_2 = \dots = m_s = 0$ et $m_1 a_1 = 0 \Rightarrow m_1 = 0$

Donc $G = G_1 \oplus \dots \oplus G_s$ $\qquad G_i$ = groupe cycliques primaires d'ordre p^{α_i}

• Unicité de la suite $(\alpha_1, \dots, \alpha_s)$

On a $G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^t\mathbb{Z})^{m_t}$

Montrons que cette décomposition est unique.

$$G[p] \simeq (\mathbb{Z}/p\mathbb{Z})[p] \times \dots \times (\mathbb{Z}/p^r\mathbb{Z})[p]$$

$$G[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times p(\mathbb{Z}/p^2\mathbb{Z})^{m_2} \times \dots \times p^{t-1}(\mathbb{Z}/p^t\mathbb{Z})^{m_t}$$

(où $G[p] = \{x \in G / px = 0\}$ = "p-groupe élémentaire de G" = groupe d'ordre p.)

Mais pour $h \leq k$ $\quad p^k(\mathbb{Z}/p^h\mathbb{Z}) = 0$. Donc :

$$p^k G \simeq p^k(\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times p^k(\mathbb{Z}/p^r\mathbb{Z})^{m_t}$$

$$\simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times (p^k\mathbb{Z}/p^r\mathbb{Z})^{m_t}$$

donc $p^k G \cap G[p] \simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}} \times \dots \times (p^k\mathbb{Z}/p^r\mathbb{Z})^{m_t}$ ⊛ } je ne vois pas pourquoi ce juillet 94 (1)

cf Alternative page suivante qui n'utilise que $p^k G$

Comme, d'autre part $(p^k\mathbb{Z}/p^{i+1}\mathbb{Z}) / (p^i\mathbb{Z}/p^{i+1}\mathbb{Z}) \simeq p^k\mathbb{Z}/p^i\mathbb{Z}$

et comme, dans un groupe commutatif $(H \times H')/(K \times K') \simeq H/K \times H'/K'$ (cf. 2.12 bouvier), on obtient :

$$p^k G \cap G[p] / p^{k+1} G \cap G[p] \simeq (p^k\mathbb{Z}/p^{k+1}\mathbb{Z})^{m_{k+1}}$$

$$\simeq (\mathbb{Z}/p\mathbb{Z})^{m_{k+1}}$$

p-groupe élémentaire. C'est donc un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$.
On voit ici qu'il est de dimension m_{k+1}. Ainsi :

$$m_{k+1} = \dim_{\mathbb{Z}/p\mathbb{Z}} \frac{p^k G \cap G[p]}{p^{k+1} G \cap G[p]}$$ qui ne dépend que de k et de G.

m_{k+1} est donc indépendant de la décomposition choisie.

Ainsi : $\quad G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^r\mathbb{Z})^{m_t} \simeq (\mathbb{Z}/p\mathbb{Z})^{m'_1} \times \dots \times (\mathbb{Z}/p^r\mathbb{Z})^{m'_{t'}}$

$(t \leq t')$

$$\Downarrow$$

$$m_1 = m'_1 \; ; \dots ; \; m_t = m'_t$$

Un argument de "cardinal" montre que $p^{m_1 + \dots + t m_t} = p^{m'_1 + \dots + t' m'_{t'}}$
donc que $(t+1) m'_{t+1} + \dots + t' m'_{t'} = 0 \Rightarrow m'_{t+1} = \dots = m'_{t'} = 0$.

CQFD

Th 2 | Soit G un groupe fini commutatif d'ordre $n = p_1^{n_1} \dots p_k^{n_k}$
G est décomposable en groupes cycliques primaires, et l'on a :

$$G \simeq \mathbb{Z}/p_1^{\alpha_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{\alpha_{12}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{\alpha_{1n_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{k1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{kn_k}}\mathbb{Z}$$

où $\begin{cases} p_1 < p_2 < \dots < p_k \\ \alpha_{i1} \leq \dots \leq \alpha_{in_i} \end{cases}$

La suite $(p_1^{\alpha_{11}}, \dots, p_1^{\alpha_{1n_1}}, \dots, p_k^{\alpha_{k1}}, \dots, p_k^{\alpha_{kn_k}})$ est parfaitement déterminé. Il se nomme "<u>le type de G</u>".

Ce théorème nous révèle la structure de tout groupe commutatif fini :
Il se démontre en utilisant le théorème de décomposition en groupes primaires

⊛ Alternative : Pourquoi parler de $G[p]$? Certains résultats restent à justifier ci-dessus au ⊛, alors utilisons seulement :

$$p^k G \simeq \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}} \times \left(p^k\mathbb{Z}/p^{k+2}\mathbb{Z}\right)^{m_{k+2}} \times \dots \times \left(p^k\mathbb{Z}/p^t\mathbb{Z}\right)^{m_t}$$

pour obtenir

$$p^kG/p^{k+1}G \simeq \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}} \times \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+2}} \times \dots \times \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_t}$$

$$\simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{m_{k+1}+\dots+m_t}$$

C'est encore un e.v. sur le corps $\mathbb{Z}/p\mathbb{Z} \doteq \mathbb{F}_p$, soit :

$$m_{k+1}+\dots+m_t = \dim_{\mathbb{F}_p}\left(p^kG/p^{k+1}G\right)$$

Cette dernière dim. est dépendante de G et de k uniquement, et l'égalité précédente permet d'obtenir successivement $m_t, m_{t-1}, \dots, m_1$ à partir de ces dimensions : l'unicité de $m_1, m_2, \dots, m_t$ est donc établie. (...)

Pour conclure, considérons encore :

$$G \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{m_1} \times \dots \times \left(\mathbb{Z}/p^t\mathbb{Z}\right)^{m_t} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{m'_1} \times \dots \times \left(\mathbb{Z}/p^{t'}\mathbb{Z}\right)^{m'_{t'}}$$

On peut toujours supposer que $t=t'$ quitte à rajouter des m_i nuls.
Vu ce qui précède, on aura :

$$\begin{cases} m_t = m'_t \\ \dots \\ m_1 = m'_1 \end{cases}$$

CQFD

$G = G(p_1) \oplus \dots \oplus G(p_k)$ (cf paragraphe II)

et en utilisant le Th 1 ci-dessus :

$$G(p_i) \simeq \mathbb{Z}/p_i^{\alpha_{i1}} \times \dots \times \mathbb{Z}/p_i^{\alpha_{in_i}}$$

L'unicité de la décomposition $(p_1^{\alpha_{11}}, \dots, p_k^{\alpha_{kn_k}})$, qui détermine le type de G, est dû :

1) à l'unicité de la suite du th. 1 : $(p_i^{\alpha_{i1}}, \dots, p_k^{\alpha_{kn_k}})$ est unique.

2) à la remarque suivante : $G = G(p_1) \oplus \dots \oplus G(p_k)$

Si G_i est p_i-primaire cyclique, alors $\forall x \in G_i \quad p_i^{\# G_i} x = 0$, donc $x \in G(p_i) = \{x \in G \,/\, p_i^{n_i} x = 0\}$. Ainsi $G_i \subset G(p_i)$

CQFD

<u>Application</u> :

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est de type $(2, 2)$

$\mathbb{Z}/4\mathbb{Z}$ est de type (2^2)

$G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$ est de type $(2^3, 2^4, 3^2, 5^3)$

Remarque : G est d'ordre $2^7 \times 3^2 \times 5^3 = 14400$ et de type $(2^3, 2^4, 3^2, 5^3)$. Le type $(2^3, 2^4, 3^2, 5^3)$ ne doit pas être confondu avec le k-uplet $(p_1^{n_1}, \dots, p_k^{n_k})$ de la décomposition de n en facteurs premiers.

Toutefois, puisque $n = \# G = \prod_{\substack{i=1,k \\ j=1,n_i}} \#\left(\mathbb{Z}/p_i^{\alpha_{ij}}\right)$, on trouve que :

$$\begin{cases} n_1 = \sum_{j=1}^{n_1} \alpha_{1j} \\ \dots \\ n_k = \sum_{j=1}^{n_k} \alpha_{kj} \end{cases} \quad \text{où } n = p_1^{n_1} \dots p_k^{n_k}$$

Co | Deux groupes abéliens finis sont isomorphes ssi ils ont même type.

preuve : Si G et G' ont même type, il est clair qu'ils sont isomorphes. Inversement si $G \simeq G'$, soit $G = \bigoplus_{i=1}^{m} \Gamma_i$ et $G' = \bigoplus_{i=1}^{m'} \Gamma_i'$ les décompositions de G et G' en groupes cycliques primaires.
$\Phi : G \xrightarrow{\sim} G'$. Alors $\bigoplus_{i=1}^{m} \Phi(\Gamma_i)$ est une décomposition de G' en groupes cycliques primaires.
D'après l'unicité des types, $m = m'$ et les types de G et de G' sont les mêmes.

A désigne une partie non vide d'un groupe G.
$N(A)=\{x\in G \,/\, xAx^{-1}=A\}$ = normalisateur de A dans G.
$C(A)=\{x\in G \,/\, \forall a\in A \quad ax=xa\}$ = centralisateur de A dans G.

a) Mq $N(A)$ est un sous-groupe de G, et que $C(A) \triangleleft N(A)$

b) Soit la relation : $x \mathcal{R} y \Leftrightarrow xax^{-1}=yay^{-1}$ (où $a\in G$ est fixé). Mq $\mathcal{R}$ est une relation d'équivalence, puis montrer que si G est fini, le cardinal de l'ensemble des conjugués de $a\in G$ est égal à l'indice du normalisateur de $\{a\}$ dans G.
(Rappel : $b\in G$ est un conjugué de a s'il existe $x\in G$ / $b=xax^{-1}$)

---

a) $e\in N(A)\cap C(A)$ donc $N(A)$ et $C(A)$ ne sont pas vides.
Si $x,y\in N(A)$, $xy^{-1}A(xy^{-1})^{-1}=xy^{-1}Ayx^{-1}=xAx^{-1}=A$ entraîne $xy^{-1}\in N(A)$, ie <u>$N(A)$ sous-groupe de G</u>.
$C(A)\subset N(A)$ et si $x,y\in C(A)$, on a : $\forall a\in A \quad axy^{-1}=xay^{-1}=xy^{-1}a$ donc $xy^{-1}\in C(A)$. <u>$C(A)$ est donc un sous-groupe de $N(A)$</u>.

* <u>$C(A) \triangleleft N(A)$</u> ?

<u>1-méthode :</u> $\forall x\in C(A) \ \forall y\in N(A) \quad yxy^{-1}\in C(A)$?

On a :

$$\forall a\in A \quad a(yxy^{-1})=ayxy^{-1}=ya'xy^{-1}=yxa'y^{-1}=yxy^{-1}a \quad \text{d'où } yxy^{-1}\in C(A)$$

(2e égalité : $yA=Ay$ donc $\exists a'\in A \,/\, ay=ya'$; 4e égalité : car $ay=ya' \Rightarrow y^{-1}a=a'y^{-1}$)

<u>2-méthode :</u> Soit $f_x\in \mathcal{S}(G)$ l'automorphisme intérieur défini par $f_x(a)=xax^{-1}$
Si $x\in N(A)$, $f_x(A)\subset A$ et l'on peut définir le morphisme de groupes :

$$\varphi : N(A) \longrightarrow (\mathcal{S}(A),\circ)$$
$$x \longmapsto f_x$$

de noyau $\operatorname{Ker}\varphi = C(A)$, donc $C(A) \triangleleft N(A)$.

b) $\mathcal{R}$ est clairement une relation d'$\sim$, et les classes d'équivalences par $\mathcal{R}$ sont en nbre égal au nbre de conjugués de a.
Comme : $x\mathcal{R}y \Leftrightarrow xax^{-1}=yay^{-1} \Leftrightarrow ax^{-1}y=x^{-1}ya \Leftrightarrow x^{-1}y\in C(\{a\})=N(\{a\})$

$G/\mathcal{R} = G/C(\{a\})$ (classes à gauche suivant $C(\{a\})$), d'où $\underbrace{\# G/\mathcal{R}}_{\text{nbre de conjugués de a}} = \underbrace{[G : C(\{a\})]}_{\text{indice de } C(\{a\}) \text{ dans } G}$.

(NB : cf VRamis ex Alg n° 2.1.10)

Soit G un groupe à 6 éléments.

a) Si G est commutatif, alors $G \simeq \mathbb{Z}/6\mathbb{Z}$

b) Si G n'est pas commutatif, alors $G \simeq \mathfrak{S}_3$

---

a) Supposons, par l'absurde, qu'il n'existe aucun élément de G d'ordre 6. L'ordre d'un élément $a \neq e$ de G sera donc 2 ou 3 (Lagrange).

* Tous les éléments de G ne peuvent être d'ordre 2 :
Sinon $H_1 = \langle a \rangle = \{e, a\}$ et $H_2 = \langle b \rangle = \{e, b\}$ permettent de parler du sous-groupe $\{e, a, b, ab\}$ d'ordre 4, et 4 ne divise pas 6. Absurde.

* Tous les éléments de G ne peuvent être d'ordre 3 :
Sinon fixons $a \in G \setminus \{e\}$ d'ordre 3, $\langle a \rangle = \{e, a, a^2\}$ et $b \in G \setminus \langle a \rangle$.
b sera d'ordre 3 et $\langle b \rangle = \{e, b, b^2\}$ vérifiera $\langle a \rangle \cap \langle b \rangle = \{e\}$
(sinon $a^2 = b^2 \Rightarrow e = b^2 a \Rightarrow b = a$ faux ; et $a = b^2 \Rightarrow ab = e \Rightarrow b = a^2$ faux car $b \in G \setminus \langle a \rangle$)
Alors $G = \{e, a, a^2, b, b^2, x\}$ et le dernier élément x ne peut qu'être d'ordre 2 (car $\langle x \rangle \cap \langle a \rangle$ sous-groupe de $\langle a \rangle$ sera d'ordre 3 ou 1 donc. Si $\# \langle x \rangle \cap \langle a \rangle = 3$, $\langle x \rangle = \langle a \rangle \Rightarrow x \in \langle a \rangle$ absurde. Donc $\# \langle x \rangle \cap \langle a \rangle = 1$ ie $\langle x \rangle \cap \langle a \rangle = \{e\}$. De m̂ pour b. Finalement $\langle x \rangle = \{e, x\}$ car $\langle x \rangle \cap \langle a \rangle = \{e\}$ et $\langle x \rangle \cap \langle b \rangle = \{e\}$)

* Finalement, il existe un élément a d'ordre 2 et un élément b d'ordre 3 dans G. Alors ab sera d'ordre 6 comme le montre le calcul :

$ab = e \Rightarrow a = b$ faux

$(ab)^2 = a^2 b^2 = b^2 \neq e$

$(ab)^3 = a \neq e$

$(ab)^4 = b \neq e$

$(ab)^5 = a b^2 \neq e$ sinon $b = a$

$(ab)^6 = e$

$\omega(ab) = 6$ est l'absurdité cherchée !

b) Tout groupe dont tous les éléments sont d'ordre 2 est commutatif (en effet : $(ab)^2 = e = a^2b^2 \Rightarrow abab = a^2b^2 \Rightarrow ba = ab$). G n'étant pas commutatif, il existe un élément $a \in G$ d'ordre 3.

Soient $\langle a \rangle = \{e, a, a^2\}$ et $b \in G \setminus \langle a \rangle$.

* Le sous-groupe H engendré par a et b a un ordre ≥ 4, donc est égal à G.
* a et b ne commutent pas, sinon $H = G$ serait commutatif.
* Si b était d'ordre 3, a^2 et b^2 seraient distincts de e, a, b, ab, ba, ce qui est absurde puisque G possède seulement 6 éléments.

Donc b est d'ordre 2.

* Comme $a^2 \notin \{e, a, b, ab, ba\}$, on en déduit $G = \{e, a, a^2, b, ab, ba\}$

puis la table :

	e	a	a^2	b	ab	ba
e	e	a	a^2	b	ab	ba
a	a	a^2	e	ab	ba	b
a^2	a^2	e	a	ba	b	ab
b	b	ba	ab	e	a^2	a
ab	ab	b	ba	a	e	a^2
ba	ba	ab	b	a^2	a	e

(Remplir les cases faciles puis s'arranger pour que tous les él. d'une ligne ou d'une colonne soient distincts !)

← d'où la fin du tableau

C'est la table de $\mathcal{S}_3$ avec :

$e = Id$ $\quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$ $\quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$

$a^2 = (1,3,2)$ etc

Soit $n \geq 3$. On désigne par $\mathcal{A}'_n$ le sous-groupe de $\mathcal{S}_n$ engendré par les cycles $(1,2,3)$, $(1,2,4)$, ..., $(1,2,n)$.

1°/ Montrer que $\mathcal{A}'_n$ est un sous-groupe de $\mathcal{A}_n$

2°/ Montrer que si i, j sont 2 entiers distincts appartenant à $\mathbb{N}_n$, les permutations $(1,2)(i,j)$ et $(i,j)(1,2)$ appartiennent à $\mathcal{A}'_n$

3°/ En déduire que $\mathcal{A}'_n = \mathcal{A}_n$. On remarquera que tte permutation σ de $\mathcal{A}_n$ s'écrit sous la forme $\sigma = \tau_1\tau_2 \ldots \tau_{2p} = \tau_1 \sigma_0 \sigma_0 \tau_2 \ldots \tau_{2p-1} \sigma_0 \sigma_0 \tau_{2p}$ où $\sigma_0 = (1,2)$ et $\tau_1, \tau_2, \ldots, \tau_{2p}$ sont des transpositions.

1°/ $\sigma_j = (1,2,j)$ est un cycle d'ordre 3. Le nombre d'orbites de σ_j est donc $p = (n-3)+1 = n-2$ et sa signature $\varepsilon(\sigma_j) = (-1)^{n-p} = (-1)^2 = 1$ ie $\sigma_j \in \mathcal{A}_n$

2°/ Supposons $i<j$.

* Si $i=1$ et $j=2$, $(i,j)(1,2) = (1,2)(i,j) = Id \in \mathcal{A}'_n$
* Si $i=1$ et $j>2$, $(1,2)(1,j) = (1,j,2) = (1,2,j)^2 \in \mathcal{A}'_n$
  $(1,j)(1,2) = (1,2,j) \in \mathcal{A}'_n$
* Si $i=2$ et $j>2$, $(1,2)(2,j) = (1,2,j) \in \mathcal{A}'_n$
  $(2,j)(1,2) = (1,j,2) = (1,2,j)^2 \in \mathcal{A}'_n$
* Si $i>2$ et $j>2$, les supports de (i,j) et $(1,2)$ sont disjoints, donc (i,j) et $(1,2)$ commutent et :

$$(1,2)(i,j) = (i,j)(1,2) = (1,2,i)(1,2,j)^2(1,2,i) \in \mathcal{A}'_n$$

3°/ Toute permutation σ de $\mathcal{A}_n$ s'écrivant $\sigma = (\tau_1\sigma_0)(\sigma_0\tau_2)\ldots(\sigma_0\tau_{2p})$ puisque $\sigma_0^2 = Id$, le 2°/ montrant que si τ est une transposition, $\tau\sigma_0$ et $\sigma_0\tau$ sont dans $\mathcal{A}'_n$, on en déduit $\mathcal{A}_n \subset \mathcal{A}'_n$. Finalement, $\mathcal{A}'_n = \mathcal{A}_n$.

---

tapé en [ugpe0004]

① E est un ensemble muni d'une loi de comp. interne associative notée multiplicativement. On suppose que :

a) $\exists e \in E \quad \forall x \in E \quad xe = x$

b) $\forall x \in E \quad \exists y \in E \quad xy = e$

Mq $(E,.)$ est un groupe

② A et B étant 2 sous-groupes d'un groupe G, soit S le sous-groupe de G engendré par $A \cup B$. a) Mq S est l'ensemble des éléments de la forme $x_1 x_2 \dots x_{2n+1}$ où $n \in \mathbb{N}$, $x_{2i} \in A$ et $x_{2i+1} \in B$ pour $i \in [0,n]$.

b) $S = AB \Leftrightarrow AB = BA$

③ Tout sous-groupe H d'indice 2 d'un groupe G est distingué.

---

① * Tout x possède un inverse (à dte et à gauche) :

Le b) assure déjà l'existence d'un inverse à droite y de x : $xy = e$

y possède aussi un inverse à droite : $\exists z \in E \quad yz = e$

Alors : $x\underbrace{yz}_{e} = ez \Rightarrow x = ez$ puis $yx = y(ez) = (ye)z = yz = e$

et y sera aussi inverse à gauche de x.

* e est élément neutre de E :

Le a) assure déjà que e est neutre à droite. On a :

$\forall x \in E \quad ex = (xy)x = x(yx) = xe = x$ d'où la conclusion.

② a) Tout groupe contenant $A \cup B$ contiendra tous les éléments de la forme $x_1 x_2 \dots x_{2n+1}$ où $x_{2i} \in A$ et $x_{2i+1} \in B$, donc $S = \{x_1 x_2 \dots x_{2n+1} / x_{2i} \in A \text{ et } x_{2i+1} \in B\}$.

Il suffit de prouver que S est un sous-groupe de G pour pouvoir affirme que S est le plus petit sous-groupe de G contenant $A \cup B$, ie le sgroupe engendré par $A \cup B$.

$S \neq \emptyset$, si $x = x_1 \dots x_{2n+1}$ et $y = y_1 \dots y_{2n+1}$ sont dans S, xy l'est aussi. Enfin,

$(x_1 x_2 \dots x_{2n+1})^{-1} = x_{2n+1}^{-1} \dots x_2^{-1} x_1^{-1}$ et $x_{2i}^{-1} \in A$, $x_{2i+1}^{-1} \in B$ donc $x^{-1} \in S$.

S est bien un sous-groupe.

b) Si $AB = BA$, les éléments $x_1 x_2 \dots x_{2n+1}$ de S s'écriront, après permutation, dans AB. Inversement, si $ab \in AB$, clairement $ab \in S$. Donc $S = AB$.

Si $S = AB$, et si $a \in A$ et $b \in B$, $ba \in S = AB \Rightarrow \boxed{BA \subset AB}$

Cette inclusion entraine que $AB \subset BA$ puisque :

$\forall a \in A \; \forall b \in B \quad b^{-1}a^{-1} \in BA \subset AB \Rightarrow \exists a' \in A \; \exists b' \in B \quad b^{-1}a^{-1} = a'b' \Rightarrow ab = b'^{-1}a'^{-1} \in BA$

(NB : Autre approche au VRamis ex Algèbre n° 2.1.18, et prolongements)

③ Soit H un sous-groupe d'indice 2 de G.

G
He = H
Hx

$G = He \overset{\cdot}{\cup} Hx$

~~On doit prouver que :~~

~~$\forall g \in G \ \forall h \in H \ \exists h' \in H \ ghg^{-1} = h'$~~

~~Par l'absurde : Si $\exists g \in G \ \exists h \in H \ ghg^{-1} \notin H$, alors $ghg^{-1} \in Hx$ et il existe $h' \in H$ tel que $ghg^{-1} = h'x$~~

~~De 2 choses l'une : * ou bien $hg^{-1} \in H \Rightarrow g^{-1} \in H \Rightarrow x = h'^{-1}ghg^{-1} \in H$ absurde~~

~~* ou bien $hg^{-1} \in Hx \Rightarrow \exists h_1 \in H \ hg^{-1} = h_1 x$ d'où $gh_1 x = h'x$~~

~~puis $gh_1 = h' \Rightarrow g = h'h_1^{-1} \in H$ ce qui est absurde car on retombe dans le 1er cas.~~

~~H sera donc distingué dans G.~~

<u>1re solution</u> : Le raisonnement direct fonctionne.

Montrons que $\forall g \in G \ \forall h \in H \quad ghg^{-1} \in H$

De 2 choses l'une : si $g \in H$, c'est évident.

si $g \in Hx$, $g = h'x$ et $ghg^{-1} = h'\underbrace{xh}x^{-1}h'^{-1}$

$xh \notin H$ (sinon $x \in H$)

donc $xh \in Hx \Rightarrow xh = h''x$

Alors $ghg^{-1} = h'h''\underbrace{x.x^{-1}}_{e}h'^{-1} \in H$ QED

<u>2e solution</u> : La plus subtile.

Les classes à droites Hx et les classes à gauche xH forment une partition de G, en 2 parties seulement, par hypothèse. Comme l'une de ces 2 parties est $H = He = eH$, on conclut évidemment : $Hx = xH$ ie $H \triangleleft G$. QED

C'est le 2-Th. d'isomorphisme (E. NOETHER). Voir Queré p 12 ou Bouvier-Richard.

Voir aussi le 2-théorème d'isomorphisme dans [cgpe0001]

Soient G un groupe et H un sous-groupe distingué de G.

1) Mq T est un sgroupe distingué de G/H ssi il est de la forme K/H où $H \subset K \triangleleft G$.
En déduire une bijection de l'ensemble des sgroupes distingués de G contenant H sur l'ensemble des sgroupes distingués de G/H.

2) Si $H \subset K \triangleleft G$, mq : $\dfrac{G/H}{K/H} \simeq G/K$

3) Application : Quels sont les sgroupes de $\mathbb{Z}/n\mathbb{Z}$? Exhiber tous les sgroupes de $\mathbb{Z}/12\mathbb{Z}$.

4) Mq H est un sgroupe distingué maximal de G ssi G/H est simple (ie ne possède pas de sgroupes distingués non triviaux)

---

1) Soit $\pi : G \longrightarrow G/H$ la proj. can. Si T est un sgroupe distingué de G/H, $\pi^{-1}(T)$ sera un sgroupe distingué de G (comme tte image réciproque d'un sgroupe distingué par un morphisme de groupe), il contient H et $\pi(\pi^{-1}(T)) = T$ (car π surjective). Si l'on pose $K = \pi^{-1}(T)$, on aura :

$$H \subset K \triangleleft G \quad \text{et} \quad T = \pi(K) = K/H$$

Réc., si $T = \pi(K)$ où $H \subset K \triangleleft G$, alors $\pi(K) \triangleleft G/H$ (c'est un résultat général : si $f : G \to G'$ est un morphisme de groupes et si $K \triangleleft G$, alors $f(K) \triangleleft f(G)$. Ici π est surjective).

* Notons : $\mathcal{G}$ = ens. des sgroupes distingués de G contenant H

$\qquad\qquad q$ = ens. des sgroupes distingués de G/H

L'application
$$\Psi : \mathcal{G} \longrightarrow q \qquad K \longmapsto \pi(K) = K/H$$
est une bijection

On vient de montrer qu'elle est surjective. Montrons son injectivité. Elle découle du résultat suivant :

$$\forall K \in \mathcal{G} \qquad \pi^{-1}(\pi(K)) = K \qquad (*)$$

On a tjrs $\pi^{-1}(\pi(K)) \supset K$, mais ici π n'est pas injective et on ne peut pas conclure rapidement à l'égalité. Mais :

$x \in \pi^{-1}(\pi(K)) \Rightarrow \pi(x) = \pi(k)$ $k \in K \Rightarrow \pi(xk^{-1}) = e \Rightarrow xk^{-1} \in H \Rightarrow x \in kH \subset K$ (car $H \subset K$). D'où (*) et l'injectivité.

2) $G/H \xrightarrow{\varphi} G/K$, $\dot{x} \longmapsto \bar{x}$ est bien définie car $\dot{x} = \dot{y} \Rightarrow xy^{-1} \in H \subset K \Rightarrow \bar{x} = \bar{y}$.

φ est un morphisme de groupes surjectif et $\ker\varphi = \{\dot{x} \in G/H \ / \ x \in K\} = K/H = \pi(K)$.

Par décomposition canonique :

$$\begin{array}{ccc} G/H & \longrightarrow & G/K \\ \downarrow & \nearrow \sim & \\ (G/H)/(K/H) & & \end{array}$$

d'où l'isomorphisme annoncé.

3) Les sgroupes de $\mathbb{Z}$ sont les $p\mathbb{Z}$; et $n\mathbb{Z} \subset p\mathbb{Z} \Leftrightarrow p \mid n$. Les sgroupes de $\mathbb{Z}/n\mathbb{Z}$ seront les $p\mathbb{Z}/n\mathbb{Z}$ où $p \mid n$. Si $n = pq$, on vérifie : $p\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z}$.

Pour $n = 12$, $\mathcal{D}_{12} = \{1, 2, 3, 4, 6, 12\}$ d'où les 6 sgroupes :

$\mathbb{Z}/12\mathbb{Z}$; $2\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{2}, \dot{4}, \dot{6}, \dot{8}, \dot{10}\} \simeq \mathbb{Z}/6\mathbb{Z}$; $3\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{3}, \dot{6}, \dot{9}\} \simeq \mathbb{Z}/4\mathbb{Z}$

$4\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{4}, \dot{8}\} \simeq \mathbb{Z}/3\mathbb{Z}$; $6\mathbb{Z}/12\mathbb{Z} \simeq \{\dot{0}, \dot{6}\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $12\mathbb{Z}/12\mathbb{Z} \simeq \{\dot{0}\}$

4) Dire que H est un sgroupe distingué maximal de G signifie que :

$$H \subset K \triangleleft G \Rightarrow K = H \text{ ou } G \qquad (*)$$

Il suffit alors d'utiliser la bijection ψ du 1) pour constater :

$$(*) \Leftrightarrow \mathcal{G} = \{\psi(H) ; \psi(G)\} = \{\{e\}, G/H\} \Leftrightarrow G/H \text{ simple}$$

<u>NB</u> : La preuve directe, qui revient à redémontrer que ψ est une bijection, est faite en $\boxed{T}$.

Soient N et M deux sous-groupes normaux (ie distingués) d'un groupe G tels que $N \subset M$. Démontrer que :

$$\left(G/N\right) / \left(M/N\right) \simeq G/M$$

$G/N = \{\dot{x} \,/\, x \in G\}$ où $\dot{x} = \dot{y} \Leftrightarrow xy^{-1} \in N$

$M/N = \{\dot{x} \,/\, x \in N\}$ (M/N a un existence indépendante de G/N, mais est isomorphe à une partie de G/N à savoir $\{\dot{x} \in G/N \,/\, x \in N\}$ (*))

$$\begin{array}{ccc} G & \longrightarrow & \left(G/N\right)/\left(M/N\right) \\ x & \longmapsto & \bar{\dot{x}} \end{array}$$

$\bar{z}$ = classe de $z \in G/N$ modulo M/N

$\dot{x}$ = " de $x \in G$ modulo N

- φ est bien défini
- φ est surjective comme composée de 2 surjections ($x \mapsto \dot{x}$ et $z \mapsto \bar{z}$)
- φ est un morphisme (comme composée de 2 morphismes de groupes)
- $x \in \operatorname{Ker}\varphi \Leftrightarrow \bar{\dot{x}} = \bar{\dot{e}} \Leftrightarrow \dot{x} \in M/N \Leftrightarrow x \in M$, donc $\operatorname{Ker}\varphi = M$.

Par décomposition canonique de φ, on constate :

$$G/M \simeq \left(G/N\right)/\left(M/N\right)$$

[(*) Une autre façon de le comprendre est d'écrire :

$G/N = \{xN \,/\, x \in G\}$

$M/N = \{xN \,/\, x \in M\}$, de constater que $M/N \subset G/N$ et que $xN \subset M \subset G$ car $N \triangleleft M$]

Soit G un groupe à 6 éléments.

a) Montrer que G possède un élément a d'ordre 2 et un élément b d'ordre 3.

b) Montrer que l'on a $ba=ab$ ou $ba=ab^2$.

En déduire que $G \simeq \mathbb{Z}/6\mathbb{Z}$ ou $G \simeq \mathfrak{S}_3$.

a)

* S'il existe un élément x de G d'ordre 6, alors $G \simeq \mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, \dot{5}\}$ contiendra $\dot{3}$ d'ordre 2 et $\dot{2}$ d'ordre 3.

* Supposons maintenant qu'aucun él. de G n'est d'ordre 6.
Tout élément x de $G\setminus\{e\}$ sera d'ordre 2 ou 3 (Lagrange)

• Si tous les él. de G sont d'ordre 2, $x^2=e$ $\forall x \in G$ entraine que G est commutatif (car $(ab)^2=e \Rightarrow abab=e \Rightarrow ba=ab$)
Si $a \neq b$ sont distincts de e, $\{e,a,b,ab\}$ sera un sous-groupe d'ordre 4 de G ce qui est absurde puisque 4 ne divise pas 6.

• Si tous les él. sont d'ordre 3, $G=\{e,a,a^2,b,b^2,c\}$ où $\langle a\rangle=\{e,a,a^2\}$ et $\langle b\rangle=\{e,b,b^2\}$, et il n'y a plus de place pour le groupe $\langle c\rangle$ engendré par c (2 sous-groupes distincts de G d'ordre 3 ne peuvent s'intercepter hors de e, car si H et H' sont de tels sous-groupes, $H\cap H'$ sera un sous-groupe de H donc d'ordre 1 ou 3 d'où $H\cap H'=\{e\}$ ou H.
Si $H\cap H'=H$, $H \subset H' \Rightarrow H=H'$ absurde)

Ccl : Il existe un élément a d'ordre 2 et un élément b d'ordre 3 dans G.

b) Ainsi $G = \{e, a, b, b^2, c, d\}$ avec $\langle a \rangle = \{e, a\}$ et $\langle b \rangle = \{e, b, b^2\}$ qui ne s'interceptent qu'en $\{e\}$ (car d'ordres 2 et 3 ...)

$ab \notin \langle a \rangle$ (sinon $b \in \langle a \rangle$)
$\notin \langle b \rangle$ (sinon $a \in \langle b \rangle$) $\} \Rightarrow$ $\boxed{ab = c}$ par exemple

De m.

$ab^2 \notin \langle a \rangle$
$\notin \langle b \rangle$ $\} \Rightarrow ab^2 \in \{c, d\}$ mais $ab^2 = c = ab \Rightarrow b = e$ absurde.

Donc $\boxed{ab^2 = d}$

$ba \notin \langle a \rangle$
$\notin \langle b \rangle$ $\} \Rightarrow ba \in \{c, d\}$ d'où 2 cas possibles : $ba = ab$ ou $ba = ab^2$

1er cas : Si $ba = ab$, $G = \{e, a, b, b^2, \overset{c}{\overbrace{ab}}, \overset{d}{\overbrace{ab^2}}\}$ sera commutatif, donc :

$(ab)^2 = b^2$
$(ab)^3 = ab.b^2 = a$
$(ab)^4 = ab.a = b$
$(ab)^5 = ab.b = ab^2$
$(ab)^6 = ab.ab^2 = e$ et ab sera d'ordre 6, donc $G \simeq \mathbb{Z}/6\mathbb{Z}$

2e cas : Si $ba = ab^2$, on construit la table de G en utilisant cette "pseudo-commutativité" et on constate l'isomorphisme entre G et $\mathcal{S}_3$:

↗	e	a	b	b^2	c ($=ab$)	d ($=ab^2$)
e	e	a	b	b^2	c	d
a	a	e	c	d	b	b^2 → vo ce lig
b	b	d	b^2	e	a	c
b^2	b^2		e	b		
c	c				e	
d	d					e

* c et d seront d'ordre 2 car :

$c^2 = (ab)^2 = \underbrace{ab.a}_{ab^2}b = a^2b^3 = a^2 = e$

$d^2 = (ab^2)^2 = ab^2ab^2 = ab.\underbrace{ba}_{ab^2}.b^2 = abab = (ab)^2 = c^2 = e$

Toute la table se complète alors en utilisant le fait que chaque ligne (resp. colonne) ne contient que des éléments distincts 2 à 2, ou en utilisant la pseudo-commutativité de a et b : $ba = ab^2$, ce qui ramène tout calcul d'un produit à une expression du style $a^\alpha b^\beta$ où $\alpha = 0$ ou 1, $\beta = 0$ ou 1 ou 2.

* L'identification à $\mathcal{S}_3$ est la suivante (par ex.) :

$e = Id$
$a = (1,2)$ $\quad c = ab = (1,2).(1,2,3) = (2,3)$
$b = (1,2,3)$ $\quad d = ab^2 = (1,2)(1,3,2) = (1,3)$
$b^2 = (1,3,2)$ $\quad$ On vérifie encore que $ba = ab^2$ ie $(1,2,3)(1,2) = (1,2)(1,3,2)$, d'où une construction de la table de $(\mathcal{S}_3, \circ)$ en tous points similaire ! . QED

réf. Ramis I.2.4

Groupes symétriques

$\mathcal{S}(E)$ = ensemble des permutations (ou substitutions) de E

$(\mathcal{S}(E), \circ)$ est un groupe appelé groupe symétrique de E

$\mathcal{S}(\mathbb{N}_n) \doteq \mathcal{S}_n$ est le groupe symétrique d'ordre n.

$\# \mathcal{S}_n = n!$

Dans toute la suite, $\# E = n$.

ex : $\mathcal{S}_3$ a 6 éléments

Id $\quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2) \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,2) \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3) \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$

τ_i = transpositions

σ_i = cycles de longueur 3

ex : Dresser la table de $\mathcal{S}_3$. Constater qu'il n'est pas abélien.

I Orbite d'un élément, transpositions, cycles

$s \in \mathcal{S}(E)$ fixé.

$x \mathcal{R} y \iff \exists k \in \mathbb{Z} \quad y = s^k(x)$ définit une relation d'équivalence.

La classe d'$\sim$ de a s'appelle l'orbite de a suivant s. On note $\mathcal{O}_s(a)$.

Un cycle est une permutation s qui ne possède qu'une et une seule orbite non réduite à 1 élément. Le cardinal de cette orbite est la longueur du cycle. Un cycle de longueur 2 est une transposition.

Le support d'une permutation s est $\operatorname{Supp} s = \{x \in E \,/\, s(x) \neq x\}$.

1°/ Etude d'un exemple

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 8 & 6 & 2 & 5 & 7 & 3 & 10 & 9 & 1 \end{pmatrix}$$

$E = \mathbb{N}_{10}$

Orbites : $\mathcal{O}_1 = \{1, 4, 2, 8, 10\}$ $\mathcal{O}_5 = \{5\}$ $\mathcal{O}_9 = \{9\}$ $\mathcal{O}_3 = \{3, 6, 7\}$

Décomposition en produit de cycles :

$$s = (1,4,2,8,10) \circ (3,6,7)$$

Décomposition en produit de transpositions :

On remarque que $(3,6,7) = (3,6)(6,7)$ d'où :

$$s = (1,4)(4,2)(2,8)(8,10)(3,6)(6,7)$$

2°/ Cas général : Théorèmes de décomposition.

Prop : Soit $\mathcal{O}$ une orbite suivant s.

1) $s(\mathcal{O}) = \mathcal{O}$

2) $\# \mathcal{O} \neq 1 \Rightarrow \forall a \in \mathcal{O} \quad s(a) \neq a$

3) $\# \mathcal{O} = p \Rightarrow \mathcal{O} = \{a, s(a), \dots, s^{p-1}(a)\}$ et $s^p(a) = a$ pour tout $a \in \mathcal{O}$.

preuve : 1) $\forall a \in \mathcal{O} \quad \mathcal{O} = \{s^k(a) / k \in \mathbb{Z}\}$. de $s(s^k(a)) = s^{k+1}(a)$ on tire $s(\mathcal{O}) \subset \mathcal{O}$. Comme s est injective et $\mathcal{O}$ fini, on conclut $s(\mathcal{O}) = \mathcal{O}$.

2) Si $s(a) = a$, $s^k(a) = a$ pour tout $k \in \mathbb{Z}$ donc $\# \mathcal{O} = 1$

3) Soit $p = \text{Inf}\{k \in \mathbb{N}^* / s^k(a) = a\}$

Par div. euclidienne, $k=pq+r$ $\quad 0\leq r<p$ $\quad$ donc $s^k(a)=s^r s^{pq}(a)=s^r(a)$

et $\mathcal{O}=\{s^r(a)\ /\ 0\leq r<p\}$.

Si $0\leq r<r'<p$, $s^r(a)=s^{r'}(a) \Longleftrightarrow s^{r'-r}(a)=a$ et de $0\leq r'-r<p$ on tire $r=r'$. Finalement :

$$\mathcal{O}=\{a, s(a),\dots, s^{p-1}(a)\}$$ est formé de p éléments distincts 2 à 2.

CQFD

Prop : Soient $\sigma_1,\dots,\sigma_k$ des cycles de supports S_i disjoints 2 à 2.

1) Les σ_i commutent 2 à 2, donc $s=\prod\limits_i \sigma_i=\sigma_1\dots\sigma_k$ est bien défini.

2) $\begin{cases} s|_{S_i}=\sigma_i \\ s|_{E\setminus \cup S_i}=Id \end{cases}$

3) Les S_i sont les orbites suivant s non réduites à 1 élément.

preuve :

1) $\sigma_i\circ\sigma_j(x)=\begin{cases}\sigma_i(x) \text{ si } x\in S_i \\ \sigma_j(x) \text{ si } x\in S_j \\ x \text{ sinon}\end{cases}$ tout comme $\sigma_j\circ\sigma_i$.

2) $\forall x\in S_i$ $\quad s(x)=\sigma_1\dots\sigma_k(x)=\sigma_i(x)$ $\quad$ car $\begin{cases}\sigma_j(x)=x & \forall x\in S_i \\ \sigma_j(\sigma_i(x))=\sigma_i(x) & \forall x\in S_i\end{cases}$

$\forall x\in E\setminus \bigcup\limits_i S_i$ $\quad s(x)=x$

3) $\forall a\in E$ $\quad \mathcal{O}_s(a)=\{s^k(a)\ /\ k\in\mathbb{Z}\}$

Si $a\in E\setminus\bigcup\limits_i S_i$ $\quad s^k(a)=a$ donc $\mathcal{O}_s(a)=\{a\}$ est réduite à 1 élément.

Si $a\in\bigcup\limits_i S_i$, par ex. $a\in S_i$, alors $s(a)=\sigma_i(a)$ d'où

$$\mathcal{O}_s(a)=\{\sigma_i^k(a)\ /\ k\in\mathbb{Z}\}=\mathcal{O}_{\sigma_i}(a)=S_i$$

CQFD

Th. Décomposition d'une permutation en produit de cycles

Toute permutation (distincte de Id) s'écrit de façon unique (à l'ordre près) comme produit commutatif de cycles de supports 2 à 2 disjoints.

preuve : $s \in \mathcal{S}(E)$

$S_1, \dots, S_k$ = orbites de s non réduites à 1 él.

$\sigma_i \doteq$ cycles de support S_i coïncidant avec s sur S_i ie tq $\begin{cases} \sigma_i|_{S_i} = s|_{S_i} \\ \sigma_i|_{E \setminus S_i} = Id_{E \setminus S_i} \end{cases}$

Les S_i étant disjoints 2 à 2, $s' \doteq \sigma_1 \dots \sigma_k$ est bien définie (cf Prop. préc.) et :

$\forall x \in S_i \qquad j \neq i \Rightarrow \sigma_j(x) = x \qquad$ d'où $s'(x) = \sigma_i(x) = s(x)$

$\forall x \in E \setminus \cup S_i \qquad \forall j \quad \sigma_j(x) = x \qquad$ d'où $s'(x) = x = s(x)$

Donc $s' = s$ et $\boxed{s = \sigma_1 \dots \sigma_k}$. La décomposition existe.

Unicité à l'ordre près : Si $\sigma_1 \dots \sigma_k = \sigma'_1 \dots \sigma'_{k'}$, les orbites devront être les m donc $k = k'$ et $S_i = S'_j$ (cf. Prop. préc.).

Si $x \in S_i = S'_j$ $\quad \begin{cases} \sigma_1 \dots \sigma_k(x) = \sigma_i(x) \\ \sigma'_1 \dots \sigma'_k(x) = \sigma'_j(x) \end{cases}$ d'où $\sigma_i = \sigma'_j$.

CQFD

De $(a_1, a_2, \dots, a_p) = (a_1, a_2)(a_2, a_3) \dots (a_{p-1}, a_p)$ on déduit :

Th : Décomposition d'une permutation en produit de transpositions

Toute permutation s de $\mathcal{S}(E)$ s'écrit comme produit de transpositions (si $n \geq 2$)

Résultat que l'on peut affiner :

Th : $\mathcal{S}_n$ ($n \geq 2$) est engendré par les transpositions $(i, i+1)$ où $1 \leq i < n$.

preuve : $1 \leq p < q < n$

(p,q) = produit de transpositions du type $(i, i+1)$?

Récurrence sur $q-p$:

* Si $q-p = 1$, c'est trivial.
* Si $q-p > 1$, $(p,q) = (q-1,q)(p,q-1)(q-1,q)$ fait aboutir la récurrence.

CQFD

3°/ Intérêt

Reprenons l'exemple du 1°/ et calculons s^{1000}.

$s = \sigma_1 \sigma_2$ où $\begin{cases} \sigma_1 = (1,4,2,8,10) & \text{est d'ordre 5.} \\ \sigma_2 = (3,6,7) & \text{est d'ordre 3} \end{cases}$

et σ_1, σ_2 commutent. D'où $s^{1000} = \sigma_1^{1000} \sigma_2^{1000} = Id . \sigma_2^{3 \times 333 + 1} = \sigma_2$.

II Signature d'une permutation

La signature de $s \in \mathcal{S}(E)$ est $\varepsilon(s) = (-1)^{n-m}$ où m est le nbre d'orbites suivant s.

$\varepsilon(Id) = 1$

τ transposition $\Rightarrow \varepsilon(\tau) = (-1)^{n-(n-1)} = -1$

σ cycle de longueur $p \Rightarrow \varepsilon(\sigma) = (-1)^{n-(n-p+1)} = (-1)^{p-1}$

s = permutation du I.1°/ $\Rightarrow \varepsilon(s) = (-1)^{10-4} = 1$

Th : $\forall s \in \mathcal{S}(E)$ $\forall \tau$ transposition $\varepsilon(s\tau) = -\varepsilon(s)$

preuve :

$\tau = \tau_{ab}$

$s' = s\tau_{ab}$

Seules les orbites suivant s contenant a ou b seront perturbées.

1er cas : <u>a et b sont dans une m̂ orbite Θ</u>

Θ est partagée en 2 orbites suivant s' :

2e cas : <u>$a \in \Theta$, $b \in \Theta'$ et $\Theta \neq \Theta'$</u>

Les 2 orbites Θ et Θ' sont recollées

Le nombre d'orbites change donc d'une unité quand on passe de s à s'.

CQFD

Co 1 : Si $s = \tau_1 \dots \tau_k$ où τ_i transposition, $\varepsilon(s) = (-1)^k$

Co 2 : $\varepsilon : (\mathcal{S}(E), \circ) \twoheadrightarrow (\{\pm 1\}, \times)$ est un morphisme surjectif de groupes.

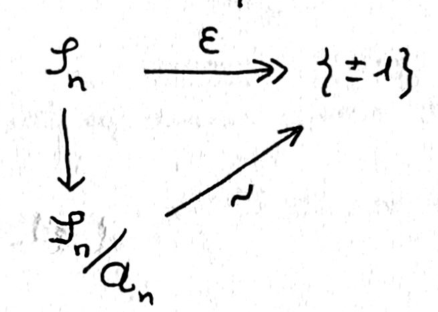
$s \longmapsto \varepsilon(s)$

preuve : Décomposer s et s' en produit de transpositions puis utiliser le Co 1 pour prouver $\varepsilon(ss') = \varepsilon(s)\,\varepsilon(s')$. La surjectivité provient de $\varepsilon(\tau) = -1$ et $\varepsilon(\tau^2) = 1$.

CQFD

Ainsi $\mathcal{A}_n \doteq \ker \varepsilon = \{ s \in \mathcal{S}_n \,/\, \varepsilon(s) = 1 \}$ est un sous-groupe distingué de $\mathcal{S}(E)$ appelé <u>groupe alterné de degré n</u>.

Par décomposition canonique de ε :



$s \in \mathcal{S}(E)$ est dite paire ou impaire suivant que $\varepsilon(s)$ vale 1 ou -1. On constate qu'il y a autant de permutations paires que impaires en écrivant :

$$\# \mathcal{S} = \underbrace{[\mathcal{S}_n : \mathcal{A}_n]}_{\doteq \, \# \mathcal{S}_n / \mathcal{A}_n = 2} . \# \mathcal{A}_n \Longrightarrow \# \mathcal{A}_n = \frac{n!}{2}$$

ex : Prouver que $\# \mathcal{A}_n = \frac{n!}{2}$ directement (Sol. : utiliser la bij. $\begin{array}{ccc} \mathcal{A}_n & \longrightarrow & \mathcal{S}_n \setminus \mathcal{A}_n \\ s & \longmapsto & \tau s \end{array}$)

> Soit φ un épimorphisme de groupes de G sur H. Soit T un sous-groupe de H.
> a) Montrer que $T \triangleleft H \Leftrightarrow \varphi^{-1}(T) \triangleleft G$
> Dans cette hypothèse, prouver que $G/_{\varphi^{-1}(T)} \simeq H/_T$
> b) Démontrer que φ induit une bijection des sous-groupes de G contenant Kerφ sur les sous-groupes de H. En déduire les sous-groupes de $\mathbb{Z}/_{n\mathbb{Z}}$.

a) * $T \triangleleft H \Leftrightarrow \varphi^{-1}(T) \triangleleft G$?

($\Rightarrow$) $\forall g \in G \quad \forall \varphi^{-1}(t) \in \varphi^{-1}(T) \quad g\varphi^{-1}(t)g^{-1} = \varphi^{-1}(\underbrace{\varphi(g)\, t\, \varphi(g)^{-1}}_{\in T}) \in \varphi^{-1}(T)$ oui

(on n'a pas utilisé la surjectivité de φ)

2ᵉ solution : $\varphi^{-1}(T) = \text{Ker}\, \pi\circ\varphi$ où $G \xrightarrow{\varphi} H \xrightarrow{\pi} H/_T$, donc $\varphi^{-1}(T) \triangleleft G$.

($\Leftarrow$) $\forall h \in H \quad \forall t \in T \quad hth^{-1} = \varphi(h_1 t_1 h_1^{-1})$ où $h = \varphi(h_1)$

$t = \varphi(t_1) \Rightarrow t_1 \in \varphi^{-1}(T) \triangleleft G$

Par hypothèse : $h_1 t_1 h_1^{-1} \in \varphi^{-1}(T) \Rightarrow hth^{-1} = \varphi(h_1 t_1 h_1^{-1}) \in T$ CQFD

(NB : Vérifier que si $\varphi : G \to H$ est un morphisme de groupes, alors 1) $T \triangleleft G \Rightarrow \varphi(T) \triangleleft \varphi(G)$ 2) $T \triangleleft H \Rightarrow \varphi^{-1}(T) \triangleleft G$)

* On obtient l'isomorphisme annoncé en décomposant canoniquement le morphisme de groupes :

$$\tilde{\varphi} : G \longrightarrow H/_T$$
$$x \longmapsto \dot{\varphi(x)}$$

$$G \downarrow \quad G/_{\varphi^{-1}(T)} \xrightarrow{\sim} H/_T$$

car $x \in \text{Ker}\tilde{\varphi} \Leftrightarrow \varphi(x) \in T \Leftrightarrow x \in \varphi^{-1}(T)$

ie $\text{Ker}\tilde{\varphi} = \varphi^{-1}(T)$

b) Soient $\mathcal{G}$ = ensemble des sous-groupes de G contenant Kerφ

$\mathcal{H}$ = " " de H.

$$\hat{\varphi} : \mathcal{G} \longrightarrow \mathcal{H}$$
$$A \longmapsto \varphi(A)$$

- L'image d'un sous-groupe par un morphisme de groupe est un sous-groupe, donc $\hat{\varphi}$ est bien définie.

- Si $T \in \mathcal{H}$, $\varphi^{-1}(T)$ est un sgroupe de G contenant $\mathrm{Ker}\,\varphi$ (car $\varphi(x) = 0 \in T \Rightarrow x \in \varphi^{-1}(T)$) et $\hat{\varphi}(\varphi^{-1}(T)) = \varphi\varphi^{-1}(T) = T$ (car φ surjective)
Cela prouve que $\hat{\varphi}$ est surjective.

- $\hat{\varphi}$ est injective car $\underset{A, B \in \mathcal{G}}{\varphi(A) = \varphi(B)} \Rightarrow \varphi^{-1}\varphi(A) = \varphi^{-1}\varphi(B) \underset{(\text{lemme})}{\Rightarrow} A = B$

|| lemme : Si $A \in \mathcal{G}$, alors $\varphi^{-1}\varphi(A) = A$
preuve : On a toujours $A \subset \varphi^{-1}\varphi(A)$. Réciproquement, si $x \in \varphi^{-1}\varphi(A)$, $\varphi(x) \in \varphi(A)$ soit $\varphi(x) = \varphi(a)$ avec $a \in A$. D'où $\varphi(xa^{-1}) = e \Rightarrow xa^{-1} \in \mathrm{Ker}\,\varphi \subset A$
$\Rightarrow x \in Aa = A$ CQFD

* Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$:

Prenons $\mathbb{Z} \overset{\varphi}{\twoheadrightarrow} \mathbb{Z}/n\mathbb{Z}$. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ seront les images des sous-groupes de $\mathbb{Z}$ contenant $\mathrm{Ker}\,\varphi = n\mathbb{Z}$, ie les $\varphi(d\mathbb{Z})$ tels que $d\mathbb{Z} \supset n\mathbb{Z}$, ie les $\varphi(d\mathbb{Z})$ avec $d | n$.

NB : $\varphi(d\mathbb{Z}) = \{\dot{x} \in \mathbb{Z}/n\mathbb{Z} \,/\, x \in d\mathbb{Z}\} \simeq d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$

Exemple : Sous-groupes de $\mathbb{Z}/12\mathbb{Z}$

On a $\mathrm{Div}(12) = \{1, 2, 3, 4, 6, 12\}$, d'où 6 sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, à savoir :

$\mathbb{Z}/12\mathbb{Z}$

$2\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{2}, \dot{4}, \dot{6}, \dot{8}, \dot{10}\} \simeq \mathbb{Z}/6\mathbb{Z}$

$3\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{3}, \dot{6}, \dot{9}\} \simeq \mathbb{Z}/4\mathbb{Z}$

$4\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{4}, \dot{8}\} \simeq \mathbb{Z}/3\mathbb{Z}$

$6\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{6}\} \simeq \mathbb{Z}/2\mathbb{Z}$

$12\mathbb{Z}/12\mathbb{Z} = \{\dot{0}\}$

LEMME D'ARTIN

Soient $\varphi_1, \dots, \varphi_m$ des morphismes de groupe, tous distincts 2 à 2, d'un groupe G vers le groupe multiplicatif F^* d'un corps F. On se donne m éléments $a_1, \dots, a_m$ de F non tous nuls en même temps.
Montrer qu'alors il existe au moins un élément g de G tel que :

$$a_1 \varphi_1(g) + \dots + a_m \varphi_m(g) \neq 0$$

(Ind. : raisonner par récurrence sur m)

---

* Si $m=1$, c'est évident, $a_1 \neq 0$ et $\varphi_1(g) \in F^*$ entraînant $a_1 \varphi_1(g) \neq 0$.

* Supposons la propriété vraie au rang $m-1$, et montrons qu'avec les hypothèses de l'énoncé :

$$\exists g \in G \qquad a_1 \varphi_1(g) + \dots + a_m \varphi_m(g) \neq 0$$

Si l'un des a_i est nul, il suffit d'appliquer l'hypothèse récurrente et c'est vrai. Si tous les a_i ne sont pas nuls, supposons par l'absurde que :

$$\forall g \in G \qquad a_1 \varphi_1(g) + \dots + a_m \varphi_m(g) = 0 \qquad (1)$$

Pour tout $h \in G$, on aura :

$$a_1 \varphi_1(hg) + \quad \dots \quad + a_m \varphi_m(hg) = 0$$

$$a_1 \varphi_1(h) \varphi_1(g) + \quad \dots \quad + a_m \varphi_m(h) \varphi_m(g) = 0$$

$$a_1 \varphi_1(h) \varphi_m(h)^{-1} \varphi_1(g) + \dots + a_m \varphi_m(g) = 0 \qquad (2)$$

En soustrayant (1) et (2), on obtient pour tout h et g dans G :

$$a_1 (1 - \varphi_1(h) \varphi_m(h)^{-1}) \varphi_1(g) + \dots + a_{m-1} (1 - \varphi_{m-1}(h) \varphi_m(h)^{-1}) \varphi_{m-1}(g) = 0$$

L'hypothèse récurrente montre que tous les coefficients des $\varphi_i(g)$ doivent être nuls :

(réf. Lidl 2.33 p59)

$$\forall i \in \mathbb{N}_{m-1} \qquad a_i \left(1 - \Psi_i(h)\,\Psi_m(h)^{-1}\right) = 0$$

d'où $\qquad \forall h \in G \quad \Psi_m(h) = \Psi_i(h)$

soit $\Psi_m = \Psi_i$, ce qui est contraire à l'hypothèse faite sur les Ψ_i .

CQFD

Montrer que 2 permutations conjuguées σ et $\tau\sigma\tau^{-1}$ ont la même parité mais pas nécessairement le même nombre d'inversions (On pourra considérer $\sigma = (1,2,3,4)$ et $\tau = (1,4)$ dans S_4)

---

* $\varepsilon(\sigma) = \varepsilon(\tau\sigma\tau^{-1})$ car $\varepsilon(\tau\sigma\tau^{-1}) = \varepsilon(\tau).\varepsilon(\sigma).\varepsilon(\tau) = \varepsilon(\sigma)$

* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ a 3 inversions tandis que $\tau\sigma\tau^{-1} = (4,2,3,1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ en a 5.

Soit D un ensemble muni d'une loi interne associative (D est un demi-groupe)

Soit $a \in D$. On considère $S = \{a, a^2, \dots, a^n, \dots\}$

a) Montrer que si S est fini, il existe 2 entiers m et n tels que $m < n$ et $a^m = a^n$.

b) n étant choisi minimum dans la relation du a), on pose $d = n - m$.

Montrer que $S = \{a, a^2, \dots, a^{n-1}\}$

c) Montrer que $C = \{a^m, \dots, a^{n-1}\}$ est un groupe cyclique (isomorphe à $\mathbb{Z}/d\mathbb{Z}$).

---

a) Si $m \neq n \Rightarrow a^m \neq a^n$ alors $S = \{a, a^2, \dots, a^n, \dots\}$ serait infini (car $\varphi : \mathbb{N} \to S$, $n \mapsto a^n$ serait injective !)

b) Soit $n = \inf\{p > m \,/\, a^m = a^p\}$. Posons $d = n - m \in \mathbb{N}^*$.

$$a^k = a^{k-n} . a^n = a^{k-n} . a^m = a^{k-(n-m)} = a^{k-d} \quad \text{dès que } k \geq n$$

ou si l'on préfère :

$$\boxed{a^k = a^{k+d} = \dots = a^{k+\nu d} \quad \forall \nu \in \mathbb{N} \quad \forall k \geq m} \qquad (*)$$

* Si $k \geq n$, notons $k = m + l$ et écrivons la div. euclidienne de l par d :

$$l = dq + r \qquad 0 \leq r < d$$

On a : $a^k = a^{m+dq+r} = a^{m+r}$ avec $m \leq m + r < m + d = n$

donc $\boxed{S = \{a, a^2, \dots, a^{n-1}\}}$

c) D'après b), le produit de 2 éléments de C sera dans C ($a^i . a^j = a^k$. Si $m \leq k \leq n-1$, on reste dans C. Sinon $k \geq n$ et $a^k = a^{m+r}$ avec $m \leq m+r < n$ comme au b)).

Le produit . est donc interne dans C.

* Les él. de C sont distincts 2 à 2 :

Si $a^k = a^{k'}$, $m \leq k < k' \leq n-1$, alors

$$a^{k+(n-k)} = a^{k'+(n-k)}$$

$$a^n = a^{n+(k'-k)}$$

$$a^{m+d} = a^{m+d+(k'-k)}$$

$$a^m = a^{m+(k'-k)} \quad \text{(cf (*) du b))}$$

absurde d'après la déf. de n, car $m < m+k'-k < n$

* Soit $\varphi : C \longrightarrow \mathbb{Z}/d\mathbb{Z}$

$$a^k \longmapsto \dot{k}$$

φ est surjective, injective (car chaque classe d'équivalence $\dot{k}$ ne possède qu'un seul représentant k dans $[m, n-1]$, et vu que les él. de C sont distincts 2 à 2)

φ est un morphisme car $\varphi(a^k a^{k'}) = \varphi(a^{k k'}) = \dot{\widehat{kk'}} = \varphi(a^k)\varphi(a^{k'})$, donc $(C, \cdot)$ est un groupe par transport de structure.

NB : Un générateur de C sera a^{m+r} où $m + r \equiv 1 \; [d]$.

H désigne un sgroupe distingué d'un groupe G. On note $\pi : G \to G/H$ l'épimorphisme canonique.

1) Mq π induit une bijection croissante de l'ensemble des sous-groupes (resp. distingués) de G contenant H sur l'ensemble des sous-groupes (resp. distingués) de G/H.

2) En déduire que <u>H est un sous-groupe distingué maximal</u> de l'ensemble des sous-groupes distingués de G distincts de G (ie $H \lhd G$ et $H \subset K \lhd G \Rightarrow K = H$ ou G) <u>ssi</u> <u>G/H est simple</u> (ie ne possède pas de sous-groupes distingués non triviaux).

(réf. résultat intéressant utilisé dans les suites de Jordan-Hölder : Queré p16)

1) π étant un morphisme de groupes, l'image directe et l'image réciproque d'un sgroupe par π sera un s-groupe. Il est de plus aisé de vérifier que :

* Si $K \lhd G$, alors $\pi(K) \lhd \pi(G) = G/H$
* Si $T \lhd G/H$ alors $\pi^{-1}(T) \lhd G$
* Si T est un sgroupe de G/H alors $\dot{e} \in T \Rightarrow \pi^{-1}(\dot{e}) = H \subset \pi^{-1}(T)$

Posons : $\mathcal{G}$ = ens. des sgroupes de G contenant H

$\mathcal{G}_d$ = " " distingués de G contenant H

$\mathcal{H}$ = ens. des sgroupes de G/H

$\mathcal{H}_d$ = " " distingués de G/H

On peut définir les applications :

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\varphi} & \mathcal{H} \\ K & \longmapsto & \pi(K) \end{array} \qquad \begin{array}{ccc} \mathcal{H} & \xrightarrow{\psi} & \mathcal{G} \\ T & \longmapsto & \pi^{-1}(T) \end{array}$$

$$\begin{array}{ccc} \mathcal{G}_d & \xrightarrow{\varphi_d} & \mathcal{H}_d \\ K & \longmapsto & \pi(K) \end{array} \qquad \begin{array}{ccc} \mathcal{H}_d & \xrightarrow{\psi_d} & \mathcal{G}_d \\ T & \longmapsto & \pi^{-1}(T) \end{array}$$

qui sont croissantes (car $K \subset K' \Rightarrow \pi(K) \subset \pi(K')$ et $T \subset T' \Rightarrow \pi^{-1}(T) \subset \pi^{-1}(T')$)

Vérifions que φ et ψ (resp. φ_d et ψ_d) sont inverses l'une de l'autre :

* π surjective entraîne $\pi(\pi^{-1}(T)) = T$

* Si K est un sgroupe de G, on a toujours $\pi^{-1}(\pi(K)) \supset K$, mais pas l'égalité en général. L'inclusion inverse provient de l'hypothèse supplémentaire $K \supset H$, comme on le voit :

$$\forall x \in \pi^{-1}(\pi(K)) \qquad \pi(x) = \pi(k) \quad \text{où } k \in K$$
$$\pi(xk^{-1}) = \dot{e}$$
$$xk^{-1} \in H$$
$$x \in Hk \subset K \quad \text{car } H \subset K$$

par suite $\pi^{-1}(\pi(K)) \subset K$ et $\pi^{-1}(\pi(K)) = K$ pour tout $K \in \mathcal{G}$ (resp. $\mathcal{G}_d$)

2) <u>H sgroupe distingué maximal de G $\Leftrightarrow$ $G/_H$ simple</u>

($\Rightarrow$) Soit $T \triangleleft G/_H$. Alors $\pi^{-1}(T) \triangleleft G$ et $H \subset \pi^{-1}(T) \subset G$ entraîne $\pi^{-1}(T) = H$ ou G, d'où $T = \pi(\pi^{-1}(T)) = \underbrace{\pi(H)}_{\{e\}}$ ou $\underbrace{\pi(G)}_{G/_H}$

$G/_H$ sera simple.

($\Leftarrow$) Soit $K \triangleleft G$ tel que $H \subset K \triangleleft G$. $\pi(K)$ est un sgroupe distingué de $G/_H$ qui est simple, donc $\pi(K) = \{e\}$ ou $G/_H$ et :

$$K = \pi^{-1}(\pi(K)) = \underbrace{\pi^{-1}(e)}_{H} \text{ ou } \underbrace{\pi^{-1}(G/_H)}_{G}$$

CQFD

> Soient G et H deux groupes cycliques. Montrer que $G \times H$ est cyclique ssi $\Delta(|G|,|H|) = 1$.

1ère solution : lemme : Soient $a \in G$ et $b \in H$. $\omega(a,b) = ppcm(\omega(a),\omega(b))$.

En effet : $(a,b)^k = (e,e') \Leftrightarrow (a^k,b^k) = (e,e') \Leftrightarrow \begin{cases} a^k = e \\ b^k = e' \end{cases} \Leftrightarrow \begin{cases} \omega(a) \mid k \\ \omega(b) \mid k \end{cases} \Leftrightarrow ppcm(\omega(a),\omega(b)) \mid k$.

Cela étant démontré, posons $\# G = m$ et $\# H = n$.

* $G \times H$ cyclique $\Rightarrow \exists (a,b) \in G \times H \quad \omega(a,b) = mn$. (a,b) engendre $G \times H$ donc a et b engendrent resp. G et H, ie sont d'ordre m et n. D'après le lemme :

$$\omega(a,b) = ppcm(m,n) = mn \qquad \text{ie} \quad m \wedge n = 1$$

* Réc., si $ppcm(m,n) = mn$ et si $G = \langle a \rangle$, $H = \langle b \rangle$, on aura :

$$\omega(a,b) = ppcm(m,n) = mn \quad \text{donc } (a,b) \text{ engendre } G \times H$$

CQFD

2ème solution : Un groupe cyclique (ie monogène fini) est un groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

On peut donc supposer que $G = \mathbb{Z}/n\mathbb{Z}$, $H = \mathbb{Z}/p\mathbb{Z}$ et tout revient à prouver que :

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \text{ cyclique} \Leftrightarrow n \wedge p = 1$$

$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ayant np élément, tout revient à montrer que :

$$\boxed{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/np\mathbb{Z} \Leftrightarrow n \wedge p = 1}$$

($\Leftarrow$) C'est le Th. Chinois.

$$\begin{array}{rcl} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \\ x & \longmapsto & (\dot{x}, \bar{x}) \end{array}$$

est un morphisme de noyau $\mu\mathbb{Z}$ où $\mu = ppcm(n,p)$ (car $\varphi(x) = 0 \Leftrightarrow x \in n\mathbb{Z} \cap p\mathbb{Z} = \mu\mathbb{Z}$)

Par décomposition canonique :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \\ \pi \downarrow & & \uparrow \\ \mathbb{Z}/\mu\mathbb{Z} & \xrightarrow{\sim} & \text{Im}\,\varphi \end{array}$$

Si $n \wedge p = 1$, $\mu = np$ et $\mathbb{Z}/\mu\mathbb{Z}$ possèdera np éléments, $\text{Im}\,\varphi$ aussi et l'inclusion

$\underbrace{\text{Im}\,\varphi}_{np \text{ él}} \subset \underbrace{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}}_{np \text{ él}}$ entraîne que φ est surjective, soit $\mathbb{Z}/np\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

($\Rightarrow$)

Supposons par l'absurde que $n \wedge p \neq 1$. Soit d un diviseur commun à n et p et distinct de 1.

$n = dn'$

$p = dp'$

$\forall u = (\dot{x}, \bar{y}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \quad dn'p'.\, u = (np'\dot{x}, pn'\bar{y}) = (\dot{0}, \bar{0})$

$$\text{donc } \omega(u) \mid dn'p'$$

Comme $dn'p' < np$, on constate que "tout élément de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/np\mathbb{Z}$ est d'ordre strictement inférieur à np". C'est absurde car $\dot{1}$ engendre $\mathbb{Z}/np\mathbb{Z}$.

QED

Un groupe abélien est dit simple s'il n'est pas réduit à son élément neutre et s'il ne possède aucun sous-groupe différent de $\{0\}$ et G. Alors :

G groupe cyclique d'ordre premier $\Leftrightarrow$ G groupe abélien simple.

($\Rightarrow$) Tout groupe cyclique est abélien. G est d'ordre p premier, donc $G \neq \{0\}$.
Enfin, si H est un sous-groupe de G, $\# H \mid \# G = p$ donc $H = \{0\}$ ou G.

($\Leftarrow$) Si $x \in G \setminus \{0\}$, G étant simple, le sous-groupe engendré par x, noté $<x>$, ne pourra être que G. Donc $G = <x>$ et <u>G est monogène</u>.
G sera donc isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$.

<u>G est fini</u> : Sinon $f : \begin{array}{l} \mathbb{Z} \to G \\ m \mapsto mx \end{array}$ est un isomorphisme, et si $p \in \mathbb{N}^* \setminus \{1\}$,
$f(p\mathbb{Z})$ sera un sous-groupe de G, ie $\{0\}$ ou G lui-même. Ce qui est absurde (car f est un isomorphisme).

<u>G d'ordre premier</u> : D'après ce qui précède, $G \simeq \mathbb{Z}/n\mathbb{Z}$. Si n était non premier, il existerait un diviseur $d \in \mathbb{N}$ de n distinct de 1 et n, et on aurait :

$$\dot{\overline{\frac{n}{d}}} \in \mathbb{Z}/n\mathbb{Z} \quad \text{et} \quad \omega\left(\dot{\overline{\frac{n}{d}}}\right) = d$$

de sorte que $< \dot{\overline{\frac{n}{d}}} >$ soit un sous-groupe d'ordre d, non trivial dans $\mathbb{Z}/n\mathbb{Z}$.

CQFD

> Montrer que toute permutation paire peut se mettre sous la forme de produit de cycles de longueur 3.
> En déduire que le groupe alterné $\mathcal{A}_n$ est engendré par les cycles $(1,2,k)$ où $3 \leqslant k \leqslant n$ (on suppose bien entendu $n \geqslant 3$ dans ces questions)

* Toute permutation paire est le produit d'un nombre pair de transpositions, soit : $\sigma = \tau_1 \tau'_1 \dots \tau_k \tau'_k$

et le produit de 2 transpositions s'exprime en fct de cycles de longueur 3 car :

$$\begin{cases} (i,j)(j,k) = (i,j,k) \\ \text{ou} \\ (i,j)(k,l) = (i,j)(j,k)^2(k,l) = (i,j,k)(j,k,l) \end{cases} \quad (\text{si } i,j,k,l \text{ distincts 2 à 2})$$

d'où le premier point.

* D'après ce qui précède, tout revient à montrer que tout cycle d'ordre 3 s'exprime en fonction des $(1,2,k)$ où $3 \leqslant k \leqslant n$.
Soit (i,j,k) avec $i < \text{Inf}(j,k)$.

- <u>1er cas : Si $i=1$</u>, on peut supposer $j \neq 2$.
  Si $k=2$, $(1,j,2) = (1,2,j)^{-1}$
  Si $k \neq 2$, $(1,j,k) = (1,2,k)^{-1}(1,2,j)(1,2,k)$

- <u>2e cas : Si $i=2$</u>, on a $(2,j,k) = (1,2,j)(1,2,k)(1,2,j)^{-1}$

- <u>3e cas : Si $i>2$</u>, on a
$$\begin{aligned}(i,j,k) &= (i,j)(j,k) \\ &= (i,j)(1,j)^2(j,k) \\ &= \underbrace{(i,j)(1,j)}_{(1,j,i)}\ \underbrace{(1,j)(j,k)}_{(1,j,k)} \\ &= (1,j,i)(1,j,k)\end{aligned}$$
qui s'écrivent en fonction des $(1,2,k)$ d'après le 1er cas.

<u>Ccl</u> : Tout él. de $\mathcal{A}_n$ s'écrit comme produit de cycles $(1,2,k)$ ou $(1,2,k)^{-1}$. Si $\mathcal{G}$ désigne le sous-groupe engendré par les cycles $(1,2,k)$, $3 \leqslant k \leqslant n$, on aura $\mathcal{A}_n \subset \mathcal{G}$.
Les cycles $(1,2,k)$ étant de signature 1, ils sont dans le groupe alterné $\mathcal{A}_n$ (des permutations paires), et l'on déduit $\mathcal{G} \subset \mathcal{A}_n$. <u>Finalement $\mathcal{G} = \mathcal{A}_n$</u>.

CQFD

Soit G un groupe de centre Z $\quad (Z = \{x \in G \,/\, \forall y \in G \;\; xy = yx\})$

a) Soit $g \in G$. Montrer que l'application $\gamma_g : \begin{array}{l} G \longrightarrow G \\ x \longmapsto gxg^{-1} \end{array}$ est un automorphisme de G. γ_g est appelé automorphisme intérieur de G.

b) Montrer que l'ensemble $\mathrm{Int}(G)$ des automorphismes intérieurs de G est un sous-groupe distingué du groupe $\mathrm{Aut}(G)$ des automorphismes de G.

c) Démontrer que $\mathrm{Int}\, G \simeq G/Z$.

---

a) $\gamma_g(xx') = gxx'g^{-1} = gxg^{-1}.\,gx'g^{-1} = \gamma_g(x).\gamma_g(x')$ montre que γ_g est un homomorphisme de G dans G. Comme $\gamma_g(x) = y \iff gxg^{-1} = y \iff x = g^{-1}yg$, on constate que γ_g est bijectif, ie un automorphisme de G.

<u>NB</u> : On constate aussi que $\gamma_g^{-1} = \gamma_{g^{-1}}$.

b) ⊛ <u>$\mathrm{Int}\, G = \{\gamma_g \,/\, g \in G\}$ est un sous-groupe de $\mathrm{Aut}(G)$ car</u> :

- $\mathrm{Id} = \gamma_e \in \mathrm{Int}\, G$
- Si $\gamma_g \in \mathrm{Int}\, G$, alors $\gamma_g^{-1} = \gamma_{g^{-1}} \in \mathrm{Int}\, G$
- Si γ_g et $\gamma_{g'}$ sont dans $\mathrm{Int}\, G$:

$$\gamma_g \circ \gamma_{g'}(x) = \gamma_g(g'xg'^{-1}) = gg'xg'^{-1}g^{-1} = gg'x(gg')^{-1} = \gamma_{gg'}(x)$$

soit $\gamma_g \circ \gamma_{g'} = \gamma_{gg'} \in \mathrm{Int}\, G$

⊛ Cette dernière relation implique que

$$\begin{array}{ccc} (G, .) & \xrightarrow{\varphi} & (\mathrm{Int}\, G, \circ) \\ g & \longmapsto & \gamma_g \end{array}$$

est un homomorphisme de groupes, surjectif par construction.

$$\mathrm{Ker}\,\varphi = \{g \in G \,/\, \forall x \in G \;\; \gamma_g(x) = x\} = Z$$ sera donc un sous-groupe distingué

ie $gxg^{-1} = x$

ie $gx = xg$

La décomposition canonique de φ donne : $\quad G/Z \simeq \mathrm{Int}\, G$ d'où c).

⊛ <u>$\mathrm{Int}\, G \lhd \mathrm{Aut}\, G$</u> est facile à montrer :

$\forall \varphi \in \mathrm{Aut}\, G \;\; \forall g \in G \quad \varphi\gamma_g\varphi^{-1}(x) = \varphi(g\varphi^{-1}(x)g^{-1}) = \varphi(g)x\varphi(g)^{-1} = \gamma_{\varphi(g)}(x)$

donc $\varphi\gamma_g\varphi^{-1} = \gamma_{\varphi(g)} \in \mathrm{Int}\, G$.

QED

a) Soit G un groupe de centre Z tel que G/Z soit cyclique, montrer que G est abélien

b) Montrer que si G est un groupe fini non abélien de centre Z, alors $\# G \geq 4 \# Z$.

---

a) Tout groupe cyclique (ie monogène fini) est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (avec $n \neq 0$) de sorte que $G/Z = \{\dot{e}, \dot{a}, \dot{a}^2, \dots, \dot{a}^{n-1}\}$

Si $x \in G$, il existe $k \in [0, n-1]$ tq $\dot{x} = \dot{a}^k$

ie $x = ca^k$ où $c \in Z$

De même, si $y \in G$, il existe $l \in [0, n-1]$ tq $y = c'.a^l$ où $c' \in Z$.

On aura :

$$xy = ca^k . c'a^l = cc' a^{k+l} = c'a^l . ca^k = yx$$

(car c et c' commutent avec tous, et $a^k.a^l = a^l a^k = a^{l+k}$)

<u>G sera commutatif</u>

b) Si $\# G < 4 \# Z$, alors $\# G/Z = \dfrac{\# G}{\# Z} < 4$ et G/Z sera cyclique (d'ordre 1, 2 ou 3). Le a) vient de montrer qu'alors G est abélien, ce qui est absurde !

Soit V la partie de $\mathcal{S}_4$ définie par :

$$V = \{ Id \ , \ (1,2)(3,4) \ , \ (1,3)(2,4) \ , \ (1,4)(2,3) \}$$

a) Montrer que V est un sous-groupe de $\mathcal{A}_4$ et que $V \triangleleft \mathcal{S}_4$.

b) Démontrer que $\mathcal{S}_4/_V \simeq \mathcal{S}_3$ et $\mathcal{A}_4/_V \simeq \mathbb{Z}/_{3\mathbb{Z}}$

Les éléments de V distincts de Id s'écrivent

$$(i,j)(k,l) \quad \text{où} \quad \{i,j,k,l\} = \{1,2,3,4\}$$

Clairement $V \subset \mathcal{A}_4$ et $(i,j)(k,l) = (k,l)(i,j)$ car ces perm. sont de supports disjoints.

a) * V est un sous-groupe :

- $V \neq \emptyset$
- Tous les produits possibles d'éléments de V (distincts de Id) sont obtenus en considérant :

$$(i,j)(k,l) \circ (i,k)(j,l) = \begin{pmatrix} i & j & k & l \\ l & k & j & i \end{pmatrix} = (i,l)(j,k) \in V$$

et $(i,j)(k,l) \circ (i,j)(k,l) = Id$

- Clairement $[(i,j)(k,l)]^{-1} = (i,j)(k,l) \in V$

NB : V est commutatif car $\forall s \in V \quad s^2 = Id$.

* $V \triangleleft \mathcal{S}_4$?

Soient $s \in \mathcal{S}_4$ et $h = (i,j)(k,l) \in V$. Il s'agit de prouver que $shs^{-1} \in V$.
On a :

$$shs^{-1} = s(i,j)(k,l)s^{-1} = \begin{pmatrix} s(i) & s(j) & s(k) & s(l) \\ s(j) & s(i) & s(l) & s(k) \end{pmatrix} = (s(i),s(j))(s(k),s(l)) \in V$$

b)

* $\# \mathcal{A}_4/V = \dfrac{\# \mathcal{A}_4}{\# V} = \dfrac{12}{4} = 3$ donc $\mathcal{A}_4/V \simeq \mathbb{Z}/3\mathbb{Z}$

* $\# \mathcal{S}_4/V = \dfrac{\# \mathcal{S}_4}{\# V} = \dfrac{24}{4} = 6$ donc $\mathcal{S}_4/V$ sera un groupe isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou à $\mathcal{S}_3$ (T).

Tout revient donc à prouver que $\mathcal{S}_4/V$ n'est pas commutatif.

<u>1-méthode</u> :

$$\underbrace{(1,2,3)}_{s}\,\underbrace{(2,4)}_{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1,2,4,3)$$

$$\underbrace{(2,4)}_{\sigma}\,\underbrace{(1,2,3)}_{s} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1,4,2,3)$$

$$\dot{s}\dot{\sigma} \neq \dot{\sigma}\dot{s} \quad \text{car} \quad s\sigma(\sigma s)^{-1} = (1,2,4,3)(1,3,2,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & & \end{pmatrix} \notin V$$

$\uparrow \uparrow$

<u>2-méthode</u> : Par l'absurde. Si $\mathcal{S}_4/V \simeq \mathbb{Z}/6\mathbb{Z}$, il existe un élément $\dot{s}$ de $\mathcal{S}_4/V$ d'ordre 6.

$$s^k = Id \Rightarrow \dot{s}^k = \dot{Id} \Leftrightarrow 6 \mid k$$

Si k est l'ordre de s, on aura $k \mid 24$ (Lagrange) et comme $6 \mid k$, on aura : $k = 6$ ou 12 ou 24.

- $k = 24$ est à exclure car $\mathcal{S}_4$ n'est pas commutatif
- $k = 12 \Rightarrow \exists\, \sigma \in \mathcal{S}_4$ d'ordre 6 (prendre $\sigma = s^2$)
- $k = 6$

Dans tous les cas, il existe une permutation σ de $\mathcal{S}_4$ d'ordre 6. C'est absurde car tout $\sigma \in \mathcal{S}_4$ s'écrit comme produit de cycles de supports disjoints, et avec 4 éléments on ne peut former aucun cycle de longueur 6 et aucun produit de cycles disjoints de longueur 2 et 3. QED

Les 2 questions peuvent être traitées indépendamment :

a) Prouver que S_n est engendré par les transpositions (i,n) où $1 \leq i \leq n-1$

b) Mq S_n est engendré par les transpositions $(i,i+1)$ où $1 \leq i \leq n-1$. En déduire que S_n est aussi engendré par les cycles $\gamma = (1,2,\dots,n-1)$ et $\tau = (n-1,n)$ (On pourra expliciter $\gamma^i \tau \gamma^{-i}$ ...)

Rappel : On sait que toute permutation σ de S_n s'écrit comme produit de cycles disjoints. Tout cycle s'écrivant comme produit de transpositions :

$$(a_1, a_2, \dots, a_k) = (a_1,a_2)(a_2,a_3)\dots(a_{k-1},a_k)$$

on en déduit que les transpositions engendrent S_n.

a) provient alors de : $$(i,j) = (i,n)(j,n)(i,n)$$

b)* Il faut écrire (i,j) comme produit de transpositions du type $(i,i+1)$ $1 \leq i \leq n-1$.
On montre que c'est possible par récurrence sur $j-i$:

H(k) : " Si $1 \leq j-i \leq k$ alors (i,j) est un produit de transpositions du type $(i,i+1)$ "

- H(1) est vraie
- Si H(k-1) est vraie, soit (i,j) avec $j-i = k > 1$.

$$(i,j) = (j,j-1)(i,j-1)(j,j-1)$$

montre que (i,j) s'écrit encore comme produit des $(i,i+1)$. QED

(NB : Une seconde démonstration est proposée en remarque à la fin de la solution)

* $\gamma = (1,2,\dots,n-1)$, $\tau = (n-1,n)$ donc $\begin{cases} \gamma(k) = k+1 \\ \gamma^2(k) = k+2 \\ \dots \\ \gamma^i(k) = k+i \end{cases}$ en posant $m = k \Leftrightarrow m \equiv k \, [n-1]$ (pour avoir $\gamma(n-1) = n = 1$)

On aura $\gamma^{-i}(k) = k-i$.
Calculons $\gamma^i \tau \gamma^{-i}(k) = \gamma^i \tau(k-i) = \tau(k-i) + i$

- Si $k-i \notin \{n-1,n\}$ ie $k \notin \{n+i-1, n+i\}$, alors $\gamma^i \tau \gamma^{-i}(k) = k$
- Si $k = n+i-1$ on a : $\gamma^i \tau \gamma^{-i}(k) = n+i$
- Si $k = n+i$ on a : $\gamma^i \tau \gamma^{-i}(k) = n+i-1$

Finalement $\gamma^i \tau \gamma^{-i} = (n+i-1, n+i) = (i, i+1)$ et ce qui précède permet de conclure.

QED

.../...

NB : On peut utiliser le a) pour prouver la 1-partie de la question b).

En effet :

<u>Par récurrence sur n</u> : $\mathcal{S}_2$ est engendré par $(1,2)$. Si $\mathcal{S}_{n-1}$ l'est par $(1,2),\dots,(n-2,n-1)$ alors tout élément de $\mathcal{S}_n$ s'écrit comme produit des (i,n) $1\leq i\leq n-1$ et :

$$(i,n) = \underbrace{(i,n-1)}\,(n,n-1)\,\underbrace{(i,n-1)} \qquad (\text{si } i<n-1)$$

s'exprime en fonction de $(1,2),\dots,(n-2,n-1)$ par hypothèse récurrente

montre que (i,n) s'exprime en fonction de $(1,2),\dots,(n,n-1)$

CQFD

Soient $(G,.)$ un groupe et x un élément de G. Notons C_x l'ensemble des éléments de G qui commutent avec x.

a) Montrer que C_x est un sous-groupe de G.

b) On appelle "centre de G", et l'on note $Z(G)$, l'ensemble des éléments qui commutent avec tous les éléments de G.
Montrer que $Z(G)$ est un sous-groupe distingué de G.

c) Vérifier que $x \in Z(G) \Leftrightarrow C_x = G$

---

a) Immédiat :
* $C_x \neq \emptyset$ car $ex = xe \Rightarrow e \in C_x$
* $\forall y \in C_x \quad yx = xy \Rightarrow xy^{-1} = y^{-1}x \Rightarrow y^{-1} \in C_x$
* $\forall y, z \in C_x \quad yzx = yxz = xyz \Rightarrow yz \in C_x$

b) * Clairement $e \in Z(G)$, donc $Z(G) \neq \emptyset$.

* $\forall x \in Z(G) \quad \forall g \in G \quad xg = gx \Rightarrow gx^{-1} = x^{-1}g \Rightarrow x^{-1} \in Z(G)$
* $\forall x, y \in Z(G) \quad \forall g \in G \quad xyg = xgy = gxy \Rightarrow xy \in Z(G)$

$Z(G)$ est donc bien un sous-groupe de G. Il est distingué(*) puisque :

$$\forall g \in G \quad \forall x \in Z(G) \qquad gxg^{-1} = gg^{-1}.x = x \in Z(G).$$

c) ($\Rightarrow$) Si x commute avec tout él. de G, on aura bien $C_x = G$.

($\Leftarrow$) Réc. $C_x = G$ signifie que $\forall g \in G \quad gx = xg$ ie $x \in Z(G)$.

(*) 2e solution : $Z(G)$ est le noyau du morphisme de groupes
$$\begin{aligned} G &\longrightarrow \mathcal{S}(G) \\ x &\longmapsto f_x(\cdot) = x . x^{-1} \end{aligned}$$
qui à tout él. x de G associe l'automorphisme intérieur f_x.
On déduit directement que $Z(G) \triangleleft G$.

|| question très bien ... .

Soient G un groupe, H un sous-groupe de G, et G/H l'ensemble des classes à gauche suivant H.
a) Montrer que G opère sur G/H par translation à gauche.
b) Montrer que pour tout x de G, le groupe d'isotropie de xH est xHx^{-1}.
c) Vérifier que le noyau K de l'action de G sur G/H est le plus grand sous-groupe distingué de G contenu dans H.
On suppose dans la suite que G est fini et H d'indice p où p est le plus petit entier divisant l'ordre de G.
d) Montrer que $[H : K]$ divise $p!$.
e) Montrer que si $q > 1$ divise $[H : K]$ alors $q \geq p$.
× f) ~~d)~~ Montrer que $H \lhd G$.)) dur !! augmenter le nombre de questions intermédiaires !

Solution :

[0] [ugps0003] Dany-Jack Mercier Licence Maths UAG 1998-99

a) G/H = ens. des classes à gauche, pour : $x R y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$
Il y a compatibilité de R et . à gauche.

$t : G \longrightarrow \mathcal{S}(G/H)$ est un homomorphisme de groupes
$g \longmapsto t_g$ où $t_g(\dot{x}) = \dot{\overline{gx}}$ car :

$\forall \dot{x} \in G/H \quad t(gg')(\dot{x}) = \dot{\overline{gg'x}} = t(g)(\dot{\overline{g'x}}) = t(g) \circ t(g')(\dot{x})$

entraine $\boxed{t(gg') = t(g) \circ t(g')}$

Donc G agit sur G/H.

b) Le sous-groupe d'isotropie de $\dot{x} = xH$ est :

$G_{\dot{x}} = \{ g \in G \,/\, t_g(\dot{x}) = \dot{\overline{gx}} = \dot{x} \}$

Donc $g \in G_{\dot{x}} \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1}$

et $\boxed{G_{\dot{x}} = xHx^{-1}}$

c)

$t_g = Id \Leftrightarrow \forall \dot{x} \ \dot{\overline{gx}} = \dot{x} \Leftrightarrow \forall \dot{x} \ g \in G_{\dot{x}} \Leftrightarrow g \in \bigcap_{x \in G} xHx^{-1}$

Donc $\boxed{K = \operatorname{Ker} t = \bigcap_{x \in G} xHx^{-1}}$

On vérifie ensuite que Ker t est le plus grand sgroupe distingué inclus dans H :

- $\operatorname{Ker} t \subset H$ puisque si $x = e$, $xHx^{-1} = H$.
- Ker t est distingué car :

$\forall y \in G \quad y(\operatorname{Ker} t)y^{-1} = y\left(\bigcap_{x \in G} xHx^{-1}\right)y^{-1} \subset \bigcap_{x \in G} \left(yx\, H\, (yx)^{-1}\right)$

$= \bigcap_{x' \in G} x'Hx'^{-1} = \operatorname{Ker} t$

• <u>Si $S \triangleleft G$ et $S \subset H$ alors $S \subset \operatorname{Ker} t$:</u>

En effet :

$$S \subset H \Rightarrow S = xSx^{-1} \subset xHx^{-1}$$

pour tout $x \in G$, donc $S \subset \bigcap_{x \in G} (xHx^{-1}) = \operatorname{Ker} t$. □

d) Par décomposition canonique de t :

$$G \xrightarrow{t} \mathcal{S}(G/H) \simeq \mathcal{S}(\mathbb{N}_{[G:H]}) = \mathcal{S}(\mathbb{N}_p)$$

$$G \to G/\operatorname{Ker} t = G/K \xrightarrow{i} \mathcal{S}(\mathbb{N}_p)$$

G/K apparaît comme isomorphe à un sgroupe de $\mathcal{S}(\mathbb{N}_p)$, donc

$$|G/K| = [G:K] \text{ divise } |\mathcal{S}(\mathbb{N}_p)| = p!$$

Il suffit de rappeler que

$$[G:K] = [G:H]\,[H:K]$$

pour constater que

$$[H:K] \mid [G:K] \mid p!$$

e) Vu l'hypothèse sur p, on peut poser

$$n = p^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{où} \quad p < p_1 < \cdots < p_k \; ; \; p, p_i \text{ premiers}$$

Si q est premier et divise $[H:K]$, alors :

$$q \mid [H:K] \mid \# H \mid \# G \Rightarrow q \mid n \Rightarrow q \in \{p, p_1, \ldots, p_k\}$$
$$\Rightarrow q \geq p$$

Si $q > 1$ divise $[H:K]$, il possède au moins un diviseur premier q_0 et on applique ce qui précède :

$$q_0 \mid [H:K] \Rightarrow q_0 \geq p \Rightarrow q \geq p.$$

β) Comme K est le plus grand sous-groupe distingué de G inclus dans **H**, montrer que $H \triangleleft G$ revient à montrer que $K = H$, ie

$$\boxed{[H:K] = 1} \qquad (*)$$

Pour montrer $(*)$, on raisonne par l'absurde. S'il existe q premier qui divise $[H:K]$, d) et e) donnent :

$$\left.\begin{array}{l} q \mid p! \\ q \geq p \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \exists k \quad q \mid k \text{ et } k \leq p \\ \quad \text{et} \\ q \geq p \end{array}\right. \Rightarrow q = p$$

Cela entraine $[H:K] = p^{\beta}$ avec $1 \leq \beta \leq \alpha$.
La question d) entraine alors : $p^{\beta} \mid p!$. Si l'on suppose $\beta > 1$, alors $p^{\beta-1} \mid (p-1)!$ entraine

$$p^{\beta-1} \equiv \underbrace{(p-1)! \equiv -1}_{\text{Th. Wilson}} \quad (p)$$

ce qui est absurde. Donc $\beta = 1$ et :

$$\boxed{[H:K] = p}$$

On en déduit :

$$[G:K] = [G:H] \times [H:K] = p^2$$

D'où (cf exercice guerre p 24, ex 24) G/K ~~cyclique~~ commutatif.

~~$G/K \simeq \mathbb{Z}/p^2\mathbb{Z}$~~

Il est alors facile de vérifier que $H \triangleleft G$, ce qui constitue l'absurdité puisqu'entraîne $H = K$. On a :

$\forall h \in H \ \forall x \in G \quad \overline{x h x^{-1}} = \dot{x} \dot{x}^{-1} \dot{h} = \dot{h}$

↑ car G/K commutatif et $K \triangleleft G$ (donc G/K est bien un gpe)

↗ Classes dans G/K

Donc :

$\forall h \in H \ \forall x \in G \quad h^{-1}.(x h x^{-1}) \in K \subset H$

$\forall h \in H \ \forall x \in G \quad x h x^{-1} \in hH = H$

(et cela signifie bien que $H \triangleleft G$.) □